SYSTEM INSTALLATION & MAINTENANCE GUIDE
FOR
BROADSWORD KEYMASTER
VERSION 2.0

● ● ● ● ●

Prepared for:

497th INTELLIGENCE GROUP
INTELLIGENCE SYSTEMS DIRECTORATE (497IG/IND)
BOLLING AIR FORCE BASE
WASHINGTON, DC 20332-5000

Prepared by:

Air Force Research Laboratory, Rome Research Site
AFRL/IFED
32 Brooks Road
Rome, NY 13441-4114

September 1999

Chapter 1
Introduction

The purpose of the System Installation & Maintenance Guide is to provide detailed procedures to install a new copy of Broadsword Keymaster Version 2.0 or to upgrade an existing Version 1.0 system. It also provides configuration information and discussion on tools provided to maintain the system.

This document is divided into three parts: (1) Installation, (2) Configuration and (3) Maintenance. The remainder of this chapter provides an overview of the Broadsword system, its architecture and functionality and an overview of the installation process.

1.1 System Overview

The Project *Broadsword* architecture is a modular, object-oriented framework which provides "data brokering," auditing, and connectivity services to heterogeneous data sources. Additional services and data sources can be added by simply "plugging in" interface modules. Using widely accepted Internet technologies, *Broadsword* aids the decision making process by querying the users data-space and returning pertinent data to the user. The major components of the system are:

- **Gatekeeper**—Provides bi-directional communication with the user interface, service interfaces, and data sources (through Data Interface Agents). The Gatekeeper also maintains system logins, user profiles, and result sets.

- **General User Interface**—Provides a method for the general user to query and retrieve results and order products. Uses a familiar browser interface for cross-platform compatibility. Also includes secure session management functionality.

1.1.1 Gatekeeper

The Gatekeeper subsystem of the *Broadsword* effort is based largely on existing Government Off-The-Shelf (GOTS) code and provides access to heterogeneous data sources. It is a robust, thin layer of software which performs a variety of internal functions, including processing users' queries; auditing usage; communicating with other Gatekeepers; maintaining system status; and collection/compilation of results. Figure 1, shows the overall architecture of the Gatekeeper. A description of each function is provided in the following paragraphs.

Project Broadsword allows the user to gather information from a variety of data sources, including structured databases and collections of free text. Any necessary query conversion is done in the plug in. A query or request can be a keyword, geo-spatial or SQL, form-based search. Once the query has been posed, the Gatekeeper forwards the query to all appropriate data sources via their plug-ins and waits for each of the sources to return.

The most important function of the Gatekeeper is the collection/collation of the query results. As individual plug-ins retrieve results from their respective data sources, the results are sent to the Gatekeeper which groups all those received for a given query. At any time, there may be several queries being processed concurrently; the Gatekeeper collates the many results for each user.
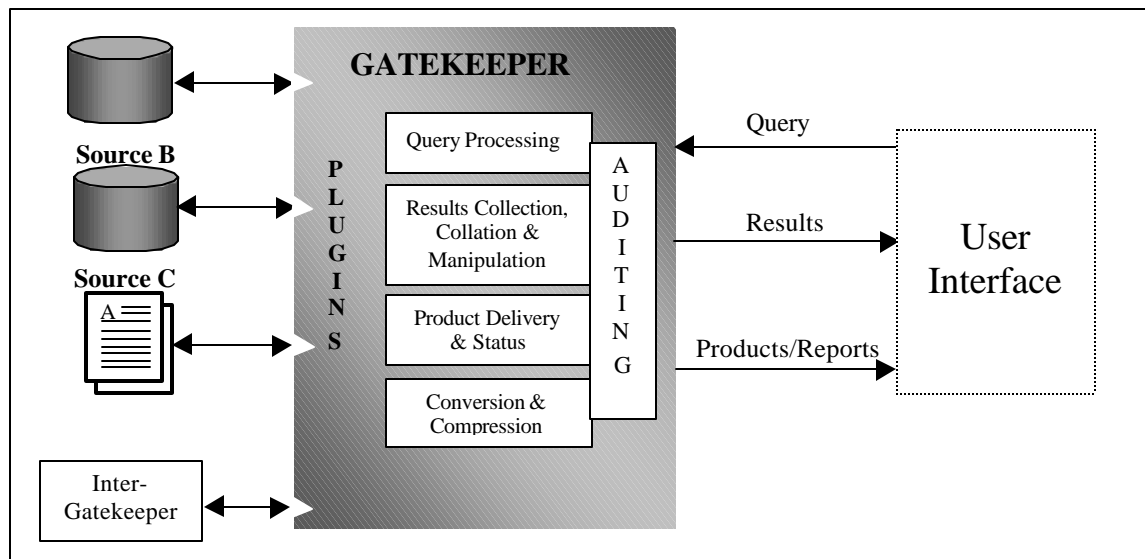
Figure 1-1 The Gatekeeper Architecture

The Gatekeeper only performs the most minimal of manipulation on the results set. It sorts the results by access_ID and flags duplicate records. Any further manipulation of results is performed by the client application. From the results list, products can be accessed on-line or (for those sources that support delivery) ordered.

A number of the sources that are connected to the Gatekeeper support the ordering or delivery of products. The Gatekeeper provides a single common mechanism to access and order products and to return the status of the order. Products include reports from database sources , messages, documents, video clips, maps and images. Delivery mechanisms from the individual sources include: tasking for non-real time mail order delivery, tasking for FTP delivery and near-real time FTP delivery.

The Gatekeeper normalizes the services provided by the imagery sources that are supported by Broadsword. It provides conversion support for NITF 2.0, NITF 1.1, Sun Raster and TIFF 6.0 and compression support for these formats.

The Gatekeeper performs all necessary security auditing. A detailed listing of all information transferred to, and received from, each user is logged. This makes it possible to review the log and

exactly determine to what information a user has had access. Table 1-1 provides a listing of the auditing events.

Security Audits	
User Events:	
Login	Product Transfer
Query	Catalog Request
Query Results	Logout
Product Request	
Administration Events:	
Gatekeeper Startup	Gatekeeper Shutdown
Add Discretionary Access Control	Delete Discretionary Access Control
Set User Discretionary Access Control	
Admin Lock	Admin Unlock
Add User	Delete User
Add Group	Delete Group
Add Group Member	
Create Source	Delete Source
Set Source Parameters	Delete Group Member
Modify Element	Clear Statistics
Register Gatekeeper	Accept Gatekeeper Registration (Keymaster Only)
Update Gatekeeper Map	
ISSO Events:	
Get Audit Report	Delete Audit Records
Dump Audit Records	Get Audit Archive List

Table 1-1 Summary of Security Audits

1.1.1.1 Connection to Sources

The Gatekeeper can connect to a source in one of two modes: (1) as a Trusted User and (2) as a Brokered User. If a source does not have the ability to support restricted access and retrieval, then the connection to the Gatekeeper will be through a trusted interface. Restriction in this sense is when the source has the ability to distinguish between users through their logins. Thus the information or view returned back is based on the user's login. A brokered login connection will maintain the user's individual login and password for that source. Table 1-2 shows the type of access provided by the Gatekeeper for the respective source.

SOURCE	ACCESS TYPE
Imagery Product Archive 1.2.3 (IPA)/Library 1.0 (IPL),	TRUSTED
Imagery Product Library 2.0 (IPL),	BROKERED
Imagery Exploitation Support System (IESS)	TRUSTED
NPIC Dissemination System (NDS)	TRUSTED
Automated Message Handling System (AMHS)	BROKERED
Imagery Dissemination Exploitation (IDEX)	TRUSTED
Military Integrated Data Base (MIDB)	TRUSTED
Demand Driven Direct Digital Dissemination (5D)	TRUSTED
Commercial Satellite Imagery Library (CSIL)	NO LOGIN REQUIRED – Registration required to order products
Space Data Base	NO LOGIN REQUIRED
Intelink (Hydra, MetaSearch)	NO LOGIN REQUIRED
Joint Intelligence Virtual Architecture (JIVA) InfoSphere Management (ISM)	
Military Equipment Parametric and Engineering Database (MEPED)	NO LOGIN REQUIRED
Air Force Weather	NO LOGIN REQUIRED

Table 1-2 Summary of Access Types

1.1.1.2 Inter-Gatekeeper Communication

Project Broadsword has the requirement to allow Gatekeepers to communicate with each other. This communication or connectivity allows users logged into one Gatekeeper to access sources connected to another Gatekeeper. Each Gatekeeper has data sources for which it is responsible. A Data Interface Agent can only access data sources attached to its hosting Gatekeeper's back-side. If it is necessary to access a data source other than those directly back-sided to your Gatekeeper, another Gatekeeper will place the query and return the results through an Inter-Gatekeeper Communication mechanism. For example, Site A's query might include a data source available at Site B. Rather than an agent from Site A accessing a data source from Site B directly, Site A's Gatekeeper communicates the query to Site B's Gatekeeper who accesses the data source and returns the results to Gatekeeper A. Gatekeeper A then collects the results, including those from Gatekeeper B, and presents them to the client.

When a new Gatekeeper wishes to join the network of Gatekeepers, it must first register itself with the "Keymaster". The process begins by the system administrator of the new Gatekeeper calling the Keymaster Distribution Center. From the Keymaster administrator a one-time registration identifier will be generated for the new Gatekeeper. The system administrator of the new Gatekeeper will then enter this registration identifier, port number of the Keymaster and the Keymaster's address into the new Gatekeeper's registration screen. At this point the new Gatekeeper will then generate a public/private key pair and send to the Keymaster a message containing: (1) its public key, the one time registration identifier and a map identifying any/all sources to be made publicly available. This map, considered the local map, is generated automatically by the gatekeeper. It identifies which sources the system administrator has allowed to be available to other sites. This is done by turning on

an option when configuring a specific source. The Keymaster, in turn will respond with a message containing: (1) a digital certificate (a timestamp, the new Gatekeeper's identification and the new Gatekeepers public key) encrypted using the Keymaster's private key, (2) a second digital certificate describing the Keymaster and (3) the world map of all other Gatekeeper's and their publicly available sources. The new Gatekeeper then stores this information for local use. At this point the Keymaster completes the registration process by sending copies of the new map to all other Gatekeepers. This is accomplished by a background process, which wakes up at a designated time, looks for any changes and sends each existing Gatekeeper the new map. Before the map is actually sent, however, an identification/authentication process takes place. This process involves the Keymaster sending its digital certificate to the given Gatekeeper. The given Gatekeeper will decrypt the certificate and respond back to the sending party (i.e., the Keymaster) its certificate.

Once each Gatekeeper is registered with the Keymaster and each have received certificates, access from one Gatekeeper to another is possible. As previously stated, the advantage of this approach is that there is no need to include the Keymaster in the requesting of a service from one Gatekeeper to another. By not having to go through the Keymaster, a single bottleneck in the architecture has been eliminated. The only time it will be necessary to include the Keymaster is when a configuration of an existing Gatekeeper has changed or a public/private key has been compromised. Figure 1-2 shows the relationship and network configuration between the Gatekeepers and the Keymaster.
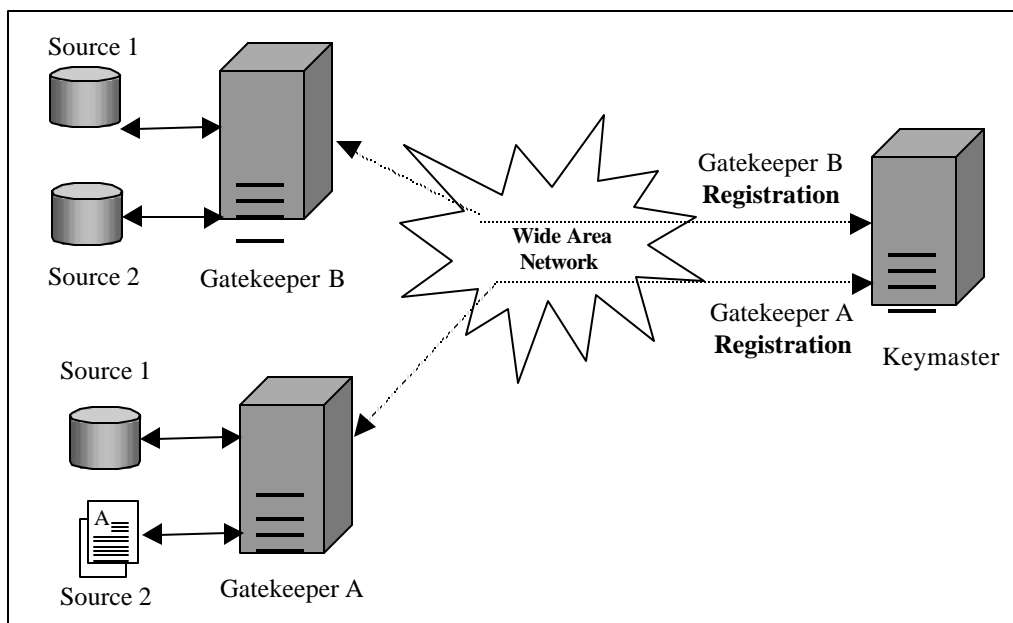
Figure 1-2 Registration Architecture

When there is a configuration change on a single Gatekeeper, it must be propagated throughout the network. Changes are accomplished through the existing system administrator screens. When changes are made they are saved into the local configuration file. At a designated time, a background process will wake up which looks at the timestamp of the file. A newer date will indicate that a change or a number of changes have been made to the Gatekeeper's configuration and that these changes must be sent to the Keymaster. After going through an identification/authentication process between the Gatekeeper and the Keymaster, the Gatekeeper sends its new configuration file up to the Keymaster. The Keymaster will acknowledge the receipt back to the Gatekeeper via a message and update its local configuration file. Again, at a designated time, the background process, at the Keymaster, will wake up, see that one of its Gatekeeper's configuration has changed and must update all Gatekeeper's with this new information. This update is performed similar to that of the initial map registration.

1.1.2 General User Interface

Project *Broadsword* provides a General User Interface to access the Gatekeeper and any attached data sources. This interface provides a robust set of tools to query, retrieve products/information, receive notification of changed information, set preferences, and order products.

The General User Interface provides a robust set of search and retrieval tools for the user. Many parameters can be configured by the user to create a customized environment for information access. The user will start from an external "Welcome" page, login with their username and password, and then have access to the main screen and functions of the interface without any further password prompts.

Since the user will be logged in before the main screen, the main screen can be tailored to give different functionality based on the "role" of each user. General users will have full access to all the Search Tools. System Administrators will have all general user functionality and System Administration functions. The Producer role combines general user functionality with the ability to catalog new information into a specified system. Each user's "role" determines which functions they have access to on their Main Screen. Figure 1-3 provides an overview of the User Interface Architecture for Project *Broadsword.*
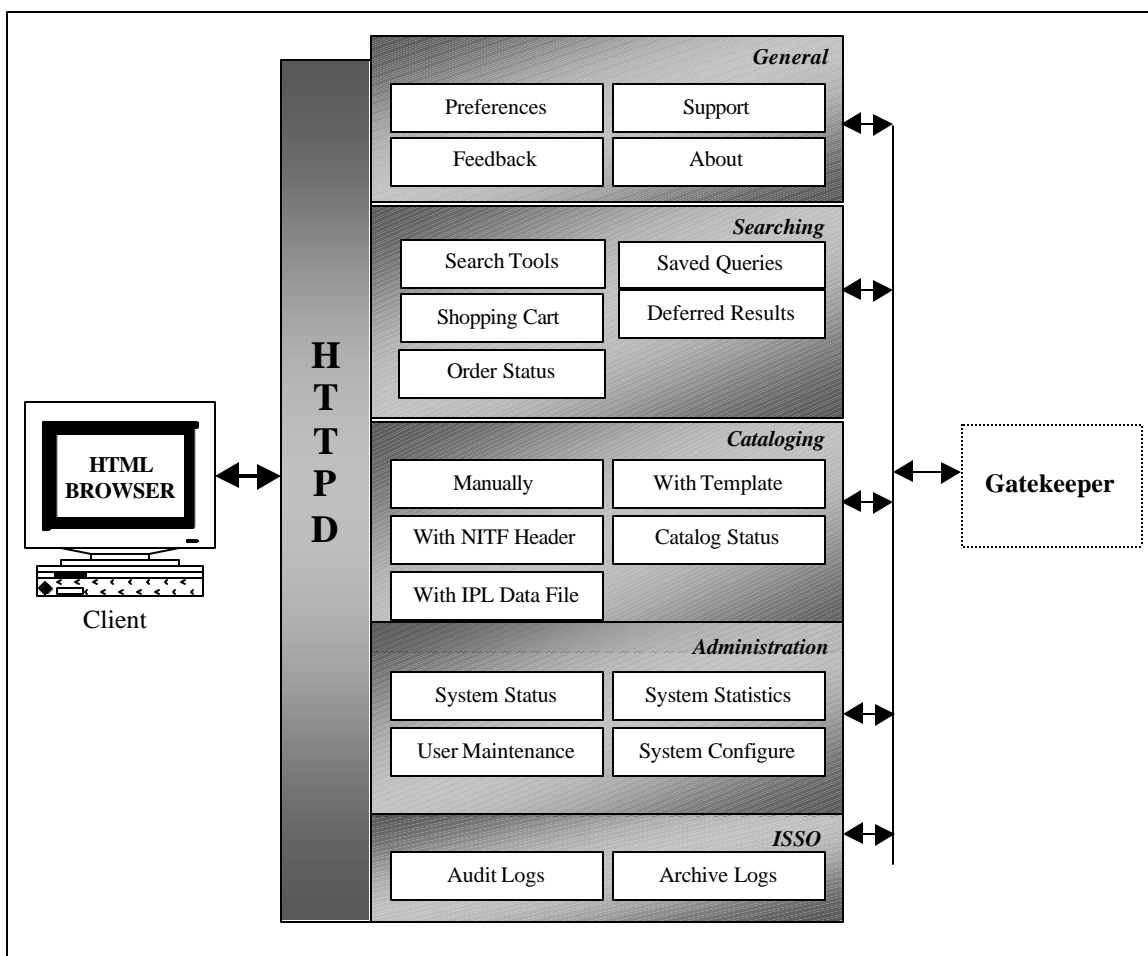
Figure 1-3 User Interface Architecture

1.1.2.1 General

The Preferences section allows the user to set up their default values and is split into six separate pages: (1) General Registration & Default First Page; (2) Information Support; (3) Delivery Options; (4) What and Where to Search and Search Utilities; (5) Attribute Configuration and (6) Remote Access. Users are able to define what their Search Tools page looks like, what data sources to search, and how. The Feedback page allows the user to provide on-line suggestions and comments about the interface. This form is pre-filled with information provided on the Preferences page. The Support page provides a listing of points of contacts for requirements, help desk, site system administration, site ISSO and site Intelink officer. The About page provides the version number of the system, and whom the current copy is registered to. These capabilities are provided to all users regardless of their privileges.

1.1.2.2 Searching

Under searching, the user is provided with tools to find, navigate and retrieve information across various sources. Searching capability is given to any user that has been given a login and password.

Searching is divided into a number of functional capabilities and is further described in the following paragraphs.

The Search Form is a user-defined page. Users are able to choose between a keyword search utility (Find), an SQL form-based utility (Query), or a spatial tool (Geographic Search). In addition users will be able to combine these search tools and configure what method they prefer through the Define Search Page preference. This preference will represent the search mechanism they use the most, and that one will be the default function accessed from the main screen. Thus, the Search Form page section is a single user-defined page, tailored to each user's preference. The results page displays all records matching the user's query. The results can be displayed as a sorted/unsorted list, timeline or on a map. There, the records can be examined further, products pulled, or products ordered. Frequently used queries can be saved through either the Search Form page or Results Page.

From the Results page, the user can either pull the information by clicking on the anchor or order the product to be delivered to a specific destination via the shopping cart. The items displayed and that are made available are dependant upon the source. Table 1-3 provides a summary of the products that are available from each source.

Source	Products Available On-Line	Supports Ordering
Imagery Product Archive 1.2.3 (IPA)/Library 1.0 (IPL),	Imagery, Video, Text Documents	Yes
Imagery Product Library 2.0 (IPL),	Imagery, Video, Text Documents, Maps	Yes
Imagery Exploitation Support System (IESS)	History of Coverage (HOC), Imagery Interpretation Reports (IIRs), Standing Requirements, Target Details	IDEX Product
NPIC Dissemination System (NDS)	None	IDEX Product
Automated Message Handling System (AMHS)	Messages	No
Military Integrated Data Base (MIDB)	Unit, Facility and Bridge Reports	No
Demand Driven Direct Digital Dissemination (5D)	Imagery	Yes
Commercial Satellite Imagery Library (CSIL)	None	Yes
Space Data Base		No
Intelink (Hydra, MetaSearch)	HTML Products	No
Joint Intelligence Virtual Architecture (JIVA) Infosphere Management (ISM)		
Military Equipment Parametric and Engineering Database (MEPED)		No
Air Force Weather	Satellite Weather Imagery	No

Table 1-3 Summary of Available Products

Currently Broadsword supports the ordering of CSIL, IPL/5D and IDEX products. There is a different process for requesting IDEX products, pulling IPL products to a destination, and ordering CSIL products. Users are able to choose several products of differing types and put them into a "shopping cart". The ordering attributes for any product placed in the cart can be modified while in the cart. Items placed in the cart can be saved from session to session and across multiple queries. At any time the user can order the items in the cart by clicking the order button. The user can find out the status of any orders that they have placed by clicking on the Order Status capability. This function provides information as to whether the product has been successfully delivered or has been shipped out (depending on the source).

The Saved Queries page provides the user with a list of all queries, which were saved through the Search Tools or Results Page, as well as functionality to process the queries in different ways. A saved query can be used interactively by the user, producing immediate results, as well as by background processing, producing deferred results. Interactive use of saved queries includes immediate execution of the query and loading of the query for display modification. Background processing of saved queries is done by the E-mail Notification and Batched Query utilities. E-mail Notification Processing periodically informs the user of new and updated products, which match the saved query. Batched Query Processing allows the user to schedule the query to be executed at a later time. The results generated by these background processing utilities are viewed through the Deferred Results Page.

The Deferred Results capability not only allows viewing of E-mail and Batched results, but also deletion of these results. For viewing, the standard display format is used to present product information, with the results summary in the upper portion of the window and the detailed hit list information in the lower portion. Deletion of E-mail results consists of removing the Product Ids from the results file. The results file, as well as the entry in the E-mail Results table, are not deleted, since the E-mail Notification is an on-going process. Deletion of Batched Results table, since batch processing is a "one-time" event.

1.1.2.3 Cataloging

The Cataloging section provides the ability to add, or "catalog", new imagery products into a specified system. This access is limited to authorized users and is currently supported only for IPL.

The cataloging capability supports the ability to automatically parse NITF 2.0 products, IPL Data Files and the generation/use of template files. It also supports the manual entry of associated metadata with the product. The format of the products is checked for valid fields based on the rules in the IPL Interface Control Document (ICD). The user can also query an available IESS and/or MIDB and automatically populate the associated fields with the information returned.

The status of whether the product has been successfully placed into the auto input queue of the appropriate IPL is provided to the user through the catalog status capability.

1.1.2.4 Administration

The System Administration (SA) section for the Gatekeeper provides system status, user maintenance, system statistics and system configuration. This access is limited to authorized users only.

System Status provides the status of all processes associated with the Project Broadsword system, the ability to turn on debug flags and maintenance for Broadsword log files.

Under User Maintenance, the system administrator grants additional privileges (i.e., system administrator, ISSO and/or Catalog) and access to various sources.

System Statistics provides Web, Gatekeeper and Batched jobs statistics. Web statistics is based on Web Usage and provides such information as the amount of bytes transferred, the top number of pages accessed and the total number of access. Gatekeeper statistics include a listing of the top N products that have been requested and how often and the top N queries.

The final section is System Configuration. Under this section, the system administrator configures the Gatekeeper, adds/removes sources, establishes site mandatory metadata fields, defines values for attributes (used for pop-downs as part of the short form) and establishes connectivity with other Gatekeepers through registration with the Keymaster.

1.2 Installation Overview

The Installation of the system consists of three major sections: (1) installation, (2) configuration and (3) removal. The purpose of the installation process is to download the software, create the database and enter the necessary configuration information to bring up an initial copy of the system. The configuration process takes this initial system and configures it by adding site specific data. The configuration process adds local sources, allows editing of system and gatekeeper values, registers the local gatekeeper with the community, configures remote sources and tailors data elements. The installation process assumes that there is a previous version of the system already installed and operational. Provided as part of the installation process is the ability to remove the older version. This process is kept separate from the actual installation since it is believed that the both versions will be run for some time until the site has the confidence that the new version has been successfully installed. At this time, the site can then execute the procedure provided at the end of Chapter 3.

IMPORTANT NOTE: Catalog status and order status have been redesigned in Broadsword 2.0, therefore, there are two notable issues that will occur while running Broadsword 1.0 when Broadsword 1.0 and Broadsword 2.0 are co-located: (1) Catalog status will always report no products cataloged; to verify that products were accepted by the IPL perform a date range (only) search. (2) Order status response is very sluggish; to verify that all products ordered have been delivered check the destination directory.

Figure 1-4 provides an outline of the procedures, which will be followed to perform the installation.

Preparing the System – Chapter 2

Server Requirements
Preparing your system

Installing the System – Chapter 3

Loading the System Software
        Providing Installation Choices
        Data Base Configuration
        Keymaster Configuration
        Client Configuration
Confirming Installation Choices
Installation Progress
Installation Verification

Configuring the System – Chapter 4 & 5

Server Configuration
        Editing/Modifying Keymaster Parameters

User Maintenance
        Editing/Modifying User Privileges
        Editing/Modifying User Accesses

Client System Requirements
        HTML Browsers

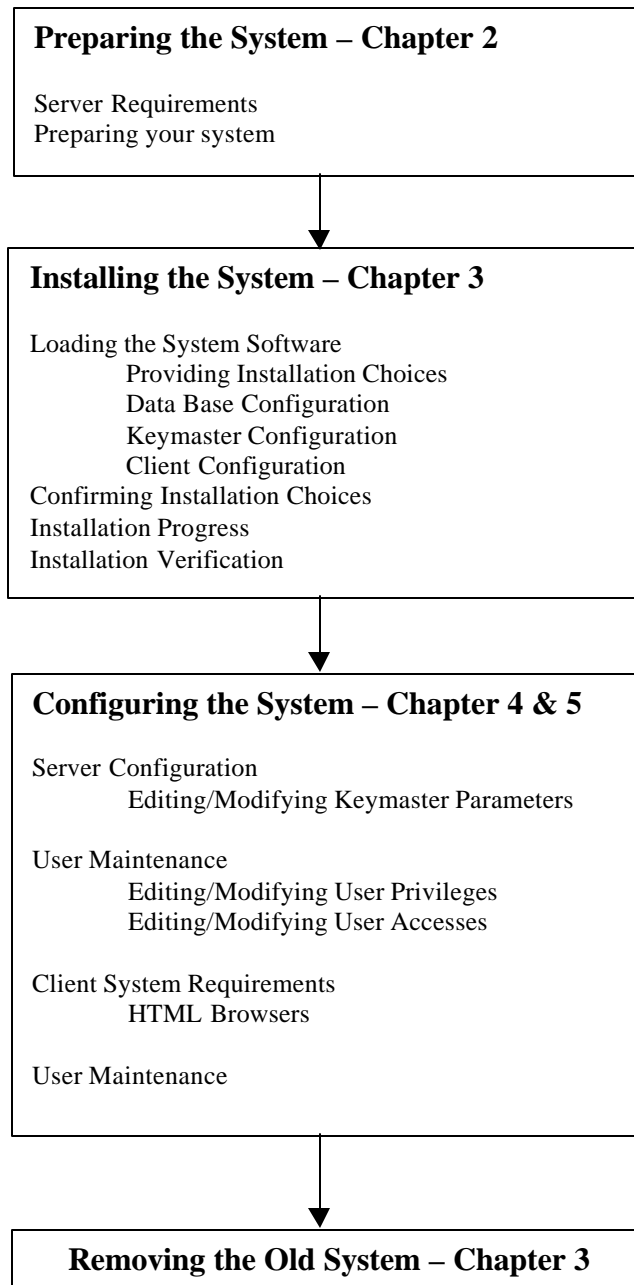User Maintenance

Removing the Old System – Chapter 3

Figure 1-4 Installation Procedure Outline

PART I

INSTALLATION

The purpose of this part is to provide detailed information to install a new version or to upgrade an existing one.

Topics covered in this part:

>   Getting Started
>>   Server Requirements
>>   Preparing your system
>>   Site Configuration Worksheet

>   Installation
>>   Loading the System Software
>>   Providing Installation Choices
>>>   Data Base Configuration
>>>   Keymaster Configuration
>>>   Client Configuration
>>   Confirming Installation Choices
>>   Installation Progress
>>   Installation Verification

>   Uninstalling the System

Chapter 2
Getting Started

The purpose of this chapter is to prepare your system for installation and to gather all the required information you'll need beforehand. At the end of this chapter is a "Site Configuration Worksheet." You should have this worksheet filled out before continuing to Chapter 3. It contains all the questions the installation script will be asking. You may want to detach it from this document to have it handy during the installation. The topics in this chapter include:

- Requirements
- Preparing Your System
- Site Configuration Worksheet

2.1   Server Requirements

Broadsword Keymaster can be installed on a dedicated Solaris system, or it can share a system with another Sybase application. Your system must be operating with at least the following hardware/software in order to successfully install and use the Broadsword Keymaster Interface:

- Solaris v2.5.1
- 4mm or 8mm Tape Drive or CD ROM Drive
- At least 1GB free disk space for Broadsword Keymaster software
- At least 2GB free disk space for Broadsword Keymaster database
- 256MB minimum/512MB recommended memory (< 5 users)
- 512MB minimum/1GB recommended memory (production system)
- X-Window Environment
- Sybase SQL Server v11.0.3.2 or above **OR** Sybase Adaptive Server v11.5 or above
- An HTML v3.2+ compliant web browser, such as Netscape 3.0+ or Internet Explorer 3.0+ (refer to Chapter 6 for more information)

Note 1: No special CSE-SS audit flags are needed for the Keymaster ; the CSE-SS minimum audits will suffice, as the Keymaster utilizes its own auditing scheme.

Note 2: Operating system patches that are recommended are those recommended by Sun Microsystems, Inc. for the particular machine model used for Keymaster. In addition, the list of Y2K-compliancy patches are as follows (Solaris 2.5.1 only):

103502-07	104093-04	104854-02
103558-10	104433-04	104857-01
103566-23	104463-02	104873-03

103612-33	104468-06	104918-01
103690-05	104490-02	104976-03
103801-06	104816-01	104977-01
103866-03	104818-01	104995-01
103876-03	104820-01	105016-01
103948-02	104822-01	105058-01
103959-05	104824-01	105124-02

Note 3: No additional operating system packages and subsets are required for the Keymaster, except those required to support CSE-SS version 1.3/1.4.

Note 4: No special steps are required to install the Keymaster in a CSE-SS environment.

2.2   Preparing your System

This section provides a list of things to do *before* installing the system.

Note: You must be user **root** at this point to perform each of the following steps (unless specified otherwise).

1 ▶ Partition Keymaster Database Devices

You must partition disk space to use for the Keymaster database, transaction log, and temp device. Use whichever utility program you normally use to partition disks, such as 'format' or 'SparcStorage Array Volume Manager', if using a Sun Sparc Disk Storage Array. The standard partition sizes are as follows, but can be made larger:

- Master Device Path: **30MB (60MB for Sybase adaptive server)**   {Worksheet #10}
- Sysprocs Device Path: 30MB**(60MB for Sybase adaptive server)**   {Worksheet #11}
- TempDevice: 100MB   {Worksheet #14-15}
- Database: 2000 MB   {Worksheet #17-18}
- Transaction Log: 500MB   {Worksheet #19-20}

You can use either raw or UNIX file system partitions for these Sybase devices, however, Sybase, Inc. recommends raw partitions. In either case, make sure that the raw device path (or UNIX directory) is owned and writeable by the Sybase user. Also be sure there is enough space available on each partition. You will be prompted during the installation for the location of these free space partitions.

Sybase licensing requires an SQL Server site license to create multiple Sybase dataservers. If your site does not have this site license, you CANNOT create multiple dataservers on this system. If this is the case, you MUST answer the question for 'Sybase Dataserver Name' (Worksheet #8) with your existing dataserver name. This will allow The Keymaster to 'share' this existing dataserver. If your site does have the site license, the installation will create a new Sybase dataserver if desired. If in question, contact your local Sybase Administrator or Sybase, Inc. at 1-800-8-SYBASE.

> **Note**: If you decide to share with an existing dataserver, be sure to choose one that has a sort order of "case - insensitive dictionary sort order." The Keymaster will not function correctly otherwise (i.e., 5D cannot be shared with because it's dataserver is case sensitive. To verify this, execute the "sp_helpsort" system stored procedure inside the dataserver in question to confirm the sort order is set as described above.

Also, if you decide to share with an existing dataserver, you will not need to partition space for a Master Device, Sysprocs Device, or Temp Device. These will be used in the existing dataserver being shared with.

2 ▶ Determine Available Disk Space

The standard location to install The Keymaster is /opt/keymaster2.0. Enter the following to determine if the /opt partition has adequate free space:

> *df -k /opt <cr>*

There should be at least 1GB available on the /opt partition. The distribution tape accounts for only a fraction of this 1GB; the rest is to allow for product & thumbnail caching. If the /opt partition doesn't contain at least 1GB of free space, you should utilize a partition that is large enough, and create a symbolic link called /opt/keymaster2.0 that points to it. For example, if the /opt partition is not large enough, but there's an /opt1 partition that is, the following commands could be used:

/usr/bin/mkdir /opt1/keymaster2.0<cr>	(Makes new directory to store Keymaster)
/usr/bin/chmod 755 /opt1/keymaster2.0<cr>	(Sets permissions)
/usr/bin/ln –s /opt1/keymasterd2.0 /opt/keymaster2.0 <cr>	(Creates symbolic link, called /opt/keymaster2.0 that "points to" /opt1/keymaster2.0)

3 ▶ Make sure *sendmail* is running on your system

In order for the Feedback and Profile Notification functions to work properly, the host on which you are installing the Interface must have *sendmail* set up. Use the following command to check if it's running:

> */usr/bin/ps -ef|grep sendmail|grep -v grep<cr>*

If you get output returned by the system, sendmail is already running, and you may proceed to the next step. If you get no output, type the following (as user root) to start sendmail:

> *sh /etc/init.d/sendmail start <cr>*

4 ▶ Perform system kernel modification, if necessary

These lines are needed by the Sybase dataserver. If the following lines don't already exist in the file /etc/system, you must append them (as user root):

> *set shmsys:shminfo_shmmax=131072000*
> *set shmsys:shminfo_shmseg=32*
> *set maxusers=512*

and issue the following commands:

> *touch /reconfigure <cr>*

> **Note**: Before issuing the following shutdown command, you must shutdown any Database
> Servers that are currently running to avoid any possible database corruption.

/usr/sbin/shutdown –y –g0 –i6 <cr>   (to reboot the system and make the new
                                                        values take effect)

5 ▶ Choose Keymaster Group

Choose an existing UNIX group on the system to use for The Keymaster, or create a new one (i.e. bswd). **All users connecting to the Keymaster Interface must be in this group**. For example, if your server already has an "ipa" group defined, and this same group of users will be allowed to connect to The Keymaster, you can simply use "ipa" as your group name. Be sure to write the group chosen in Field (24) in the Site Configuration Worksheet below.

6 ▶ Create Keymaster System Administration User

Create a new UNIX user on the system, using your normal means, called *bswduser*. This user will be used for System Administration functions. Add this user to the Keymaster group chosen or created above.

7 ▶ Complete the Site Configuration Worksheet (below)

After correctly completing the above steps, fill out the **ENTIRE** worksheet below, as you will refer to it during the installation process in Chapter 3.

2.3   Site Configuration Worksheet

The following section previews all the configuration questions that will be asked during the installation process. You are encouraged to write in your answers on this page so that you have them handy during installation. (The numbers adjacent to the Field Names are referred to throughout this guide.)

> **Note:** For completeness, password fields are listed here. However, it is advisable NOT to write down any passwords on this sheet. You should remember them.

Field Number	Field Name	Your Answer	Description
1	Install Mode Selection		Install Mode preferences (Default: New Install)
2	Keymaster Previous Version Path		Path to previous version of Keymaster. Asked only if Install Mode is upgrade
3	Dataserver Creation Method		Dataserver Creation Method (Default: Create New)
4	Sybase Username		Sybase UNIX username associated with version of Sybase being used for Keymaster. (Default: Sybase)
5	Sybase Home Dir Path		Home directory path of Sybase SQL Server or Sybase Adaptive server.
6	Sybase Dataserver Name		The dataserver name to create or share for Keymaster Sybase server. (Default: KM_<hostname>_SVR)
7	Sybase Dataserver Port Number		UNIX port to be used by the Keymaster Sybase server. Asked only if creating a new dataserver. (Default: 2502)
8	Sybase Dataserver Master Device Path		System location to place Keymaster dataserver master device. Can either be a raw device (i.e. /dev/rdsk/c0t1d0s2), highly recommended, or a standard UNIX file path, such as /opt/bswd_syb_devices. Must be at least 30MB free on path (60 MB for Sybase Adaptive Server). Asked only if creating a new dataserver.
9	Sybase Dataserver Sysprocs Device Path		System location to place Keymaster dataserver systemprocs device. Can either be a raw device (i.e. /dev/rdsk/c0t1d0s2), highly recommended, or a standard UNIX file path, such as /opt/bswd_syb_devices. Must be at least 30MB free on path (60 MB for Sybase Adaptive Server). Asked only if creating a new dataserver.
10	Sybase B/U Server Create?		Create new Sybase Backup Server? Asked only if creating a new dataserver. If a Sybase Backup Server already exists on this system, you may click "No".
11	Sybase B/U Server Port #		UNIX port to be used by the Sybase Backup Server. Asked only if creating a new dataserver, and "Yes" is answered to question above.
12	Keymaster TempDevice Path		System location to place Keymaster TempDevice. Can either be a raw device (i.e. /dev/rdsk/c0t1d0s2), highly recommended, or a standard UNIX file path, such as /opt/bswd_syb_devices. Asked only if creating a new dataserver.
13	Keymaster TempDevice Size		Size to make the Keymaster TempDevice. Asked only if creating a new dataserver. (Default: 100MB)
14	Sybase Administrator Password	(don't write here)	The password for the Sybase System Administrator (sa). Asked only if sharing an existing dataserver.

Field Number	Field Name	Your Answer	Description
15	Keymaster Data Device Path		System location to place Keymaster database. Can either be a raw device (i.e. /dev/rdsk/c0t1d0s2), highly recommended, or a standard UNIX file path, such as /opt/keymaster_syb_devices.
16	Keymaster Data Device Size		Size to make the Keymaster database. (Default: 2000 MB)
17	Keymaster Log Device Path		System location to place Keymaster database transaction log. Can either be a raw device (i.e. /dev/rdsk/c0t1d0s2), highly recommended, or a standard UNIX file path, such as /opt/keymaster_syb_devices.
18	Keymaster Log Device Size		Size to make the Keymaster database transaction log. (Default: 500 MB)
19	bswduser Account Password	(don't write here)	UNIX password for 'bswduser' account created in Chapter 2.
20	Server Type		Server type for this Keymaster Installation. (Choices: Protected or Both Protected and Registered)
21	Protected HTTP port #		UNIX port to be used by the Protected HTTP daemon.
22	Network host machine is on		Network type host machine is connected to. (Choices: SIPRNET; JWICS; or Internet) (Default: SIPRNET)
23	SIPRNET Project Broadsword Program Office IP Address		IP Address (on Intelink-S only) of Project Keymaster Program Office homepage. Asked only if network type is SIPRNET. If this address is unknown contact the Broadsword Program Office at (315) 330-1629.
24	Group Name		UNIX group to use for Keymaster
25	System Admin Name		System Administrator name (MANDATORY)
26	System Admin Branch		System Administrator branch (MANDATORY)
27	System Admin Organization		System Administrator organization (MANDATORY).
28	System Admin Address1		System Administrator address (MANDATORY).
29	System Admin Address2		System Administrator address (MANDATORY).
30	System Admin Phone		System Administrator UNCLASSIFIED phone number (MANDATORY).
31	System Admin FAX		System Administrator FAX (MANDATORY)
32	System Admin E-mail		System Administrator E-mail (MANDATORY)
33	System Admin City		System Administrator City (MANDATORY)
34	System Admin State/Locality		System Administrator State/Locality (MANDATORY)
35	System Admin Country Code		System Administrator Country Code (MANDATORY)

Field Number	Field Name	Your Answer	Description
36	ISSO Name		ISSO name.
37	ISSO Branch		ISSO branch.
38	ISSO Organization		ISSO organization.
39	ISSO Address1		ISSO address.
40	ISSO Address2		ISSO address.
41	ISSO Phone		ISSO UNCLASSIFIED phone number.
42	ISSO Fax		ISSO fax number.
43	ISSO Email		ISSO email address.
44	Intelink Site Info Manager Name		Intelink Site Information Manager name.
45	Intelink Site Info Manager Branch		Intelink Site Information Manager branch.
46	Intelink Site Info Manager Organization		Intelink Site Information Manager organization.
47	Intelink Site Info Manager Address1		Intelink Site Information Manager address.
48	Intelink Site Info Manager Address2		Intelink Site Information Manager address.
49	Intelink Site Info Manager Phone		Intelink Site Information Manager UNCLASSIFIED phone number.
50	Intelink Site Info Manager Fax		Intelink Site Information Manager fax number.
51	Intelink Site Info Manager Email		Intelink Site Information Manager email address.

Table 2-1 Site Configuration Worksheet

Chapter 3
Installation

The purpose of this chapter is to provide detailed procedures to install the basic server software. It covers both a new install and an upgrade to an existing one. Whether this is a new install or an upgrade make sure you have completed Chapter 2 first. After completing the instructions provided within you must proceed to Chapter 4 to configure and tailor the system. Specific topics covered include:

- Loading the Software and Starting the Install Script
- Providing Installation Choices
- Confirming Installation Choices
- Configuration Progress
- Installation Verification
- Uninstalling the System (Current or Previous Version)

3.1 Loading the Software and Starting the Install Script

1 Start a terminal window (xterm shell):

At the command line type:
/usr/openwin/bin/xterm <cr>

or launch a Terminal window off the desktop. You may want to launch two windows just in case you might want to monitor some part of the process or need to look something up during the process.

2 Within this new window login as super-user on the machine you wish to install:

su - root <cr>

3 Insert the distribution CD into the CD-ROM drive.

At the shell prompt, enter:
cd /cdrom/cdrom0 <cr>

4 Execute the install script:

The execution format of the install script is as follows:

Usage: ./install.sh
        -display display_name
        -sybase sybase_dir
        [-s source_path] (Default: /cdrom/cdrom0)
        [-d dest_path]   (Default: /opt/keymaster2.0)
        [-nountar]   (Do not extract Keymaster tar files)

        Where:
                <display_name> is the X display name that you are installing from (where the install GUI will be displayed) [i.e. bianica:0.0].

                <sybase_dir> is the directory where the Sybase product is located (refer to Worksheet #5 in the previous chapter) [i.e. /opt/SYBASE].

                <source_path> is the directory in which the Keymaster distribution tar files are stored [defaults to /cdrom/cdrom0 if –s not specified].

                <dest_path> is the directory in which you would like Keymaster software to be installed [defaults to /opt/keymaster2.0 if –d not specified].

                <-nountar> is specified only in cases where the Keymaster distribution tar files have already been extracted (i.e. the tar files have already been extracted fully, and there is just a need to start over at the install GUI).

An example of executing the script would be: **./install.sh –display bianica:0.0 -sybase /opt/SYBASE <cr>**

3.2   Providing Installation Choices

After the install script has successfully extracted the two tar files, it will launch the graphical portion of the install process. This portion will take the installer step by step through the remainder of the installation process. Figure 3-1 shows the initial screen .
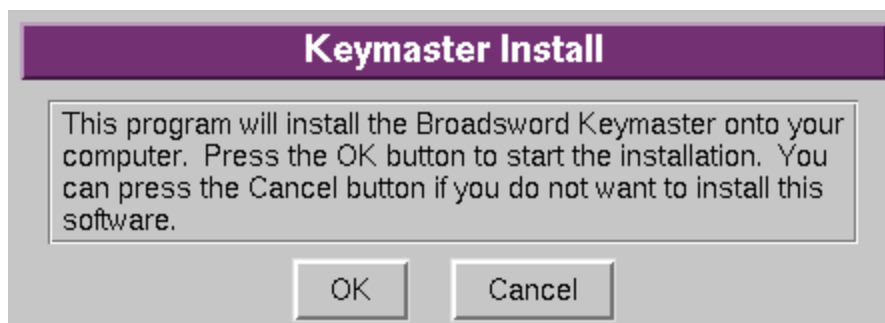

Figure 3-1 Initial Installation Screen

3.2.1 Determining the Install Mode

After clicking the "OK" button the installer is asked whether this will be a new install or an upgrade to an existing Keymaster system. Either mode will install the software in such a manner that it will not destroy the existing system. Upgrade Mode imports user files and existing configuration files (i.e., registered gatekeepers) from the previous version specified. Figure 3-2 shows this screen. For a new install the upgrade path will be ignored.
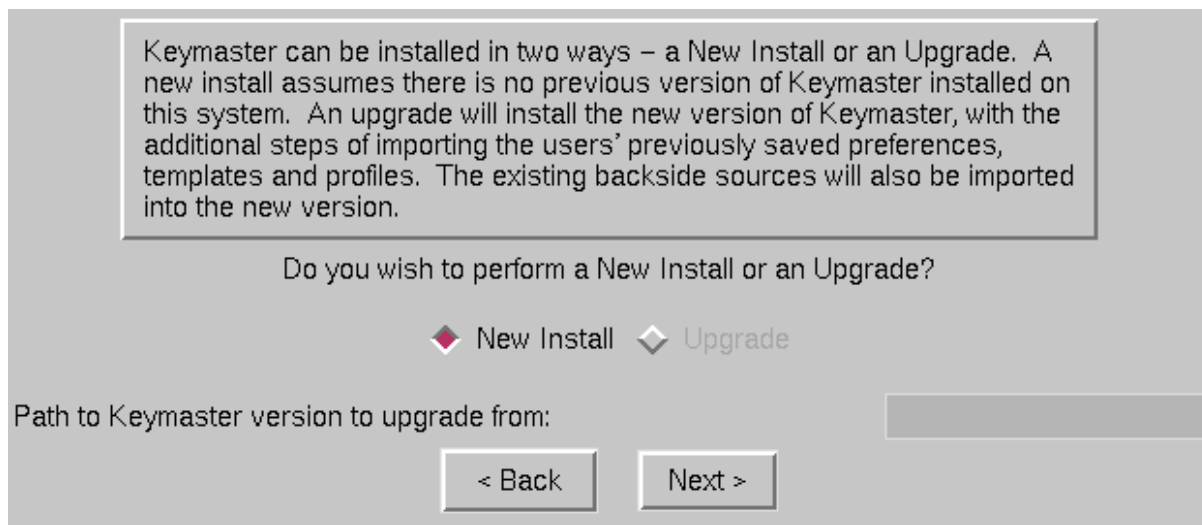

Keymaster can be installed in two ways – a New Install or an Upgrade. A new install assumes there is no previous version of Keymaster installed on this system. An upgrade will install the new version of Keymaster, with the additional steps of importing the users' previously saved preferences, templates and profiles. The existing backside sources will also be imported into the new version.

Do you wish to perform a New Install or an Upgrade?

◆ New Install ◇ Upgrade

Path to Keymaster version to upgrade from:

< Back   Next >

Figure 3-2 New Install versus Upgrade Screen

FIELDS VALIDATED	
Upgrade Path (Previous version)	File <Path Entered>/client/bin/keymaster EXISTS AND <Path Entered> != current version being installed.

Table 3-1 Fields Validated

3.2.1.1 Data Base Configuration

After clicking the "Next" Button, the install script asks whether the database will exist as a separate Data Server or share the existing server. Each Data Server requires their own license. If a site has a site license for Sybase, then both options are available to the site. **Note:** The existence of Sybase licenses is **NOT** determined automatically by the installer; it is up to the site personnel to determine this. If the site has only a single server license, the only option available to the site is to install the Data Base under the existing Data Server. The disadvantage of using a shared Data Server is that if it goes down for some reason, all the Data Bases running under the Data Server will go down.   This becomes a reliability concern.

3.2.1.1.1 Creating a New Data Server

Figure 3-3 provides a sample of this screen. The default option is to "Create new". If the "Share existing" option is picked, skip to Section 3.2.1.1.2.

Figure 3-3 "Creating the Data Server" Screen

If the "Create new" option is chosen (as shown in Figure 3-4), the installation process will next ask for information required to configure the Data Server.

Figure 3-4 Initial Data Base Configuration Screen

A number of default values have been entered. The installer must verify these values along with entering the additional requested information. The additional requested information specifically identifies where Sybase will physically write its data. The device path can be either a path to a raw partition or a file system. Figure 3-5 shows the sample screen with the device paths filled in and the creation of a SYBASE Backup Server.

Note: The new dataserver created will have an administrator (sa) password that is empty. To set a password please refer to Appendix C.

Figure 3-5 Example Data Base Configuration Screen

FIELDS VALIDATED	
Sybase Username	Username entered exists on system.
Sybase Home Directory Path	File <Path Entered>/bin/dataserver EXISTS.
Sybase Dataserver Name	Name entered is a currently defined dataserver (when in sharing mode). Also, when in sharing mode, verifies that dataserver entered is running.
Sybase Administrator Password	Installer enters it twice AND password is verified by doing test login into dataserver.
Dataserver Port #	Port number is not already in use.
Master Device Path	Path EXISTS AND is writable by the Sybase User entered earlier AND there is enough space available for device (30 or 60 MB).
Sysprocs Device Path	Path EXISTS AND is writable by the Sybase User entered earlier AND there is enough space available for device (30 or 60 MB).
Backup Server Port #	Port number is not already in use.

Table 3-2 Fields Validated

After entering the requested information and pressing the "Next" button, the install process asks for information to configure the temporary device for Sybase only if creating a new dataserver.
Figure 3-6 provides an example of this screen with both the path and size entered.

Figure 3-6 Sample "TempDevice Configuration" Screen

The next step in the installation process is to configure the Sybase Data and Log Devices. Similar information as with the Temporary Device portion is requested. Figure 3-7 provides an example of this screen.

Figure 3-7 Sample "Database Configuration" Screen

FIELDS VALIDATED	
Data Device Path	Path EXISTS AND is writable by the Sybase User entered earlier AND there is enough space available for device.
Log Device Path	Path EXISTS AND is writable by the Sybase User entered earlier AND there is enough space available for device.

Table 3-3 Fields Validated

At this point all the necessary information to configure the Data Server is complete. The installation process will next request information needed to configure the Keymaster. Skip to section 3.2.1.2, below to proceed with the installation.

3.2.1.1.2 Sharing the Existing Data Server

If the "Share existing" option is chosen, as shown in Figure 3-8, the installation process will next ask for information required to configure the Data Base.

Figure 3-8 "Sharing the Existing Data Server" Screen

A number of the default values have been entered. The installer must verify these values along with entering the additional requested information. The additional requested information specifically identifies where Sybase will physically write its data. Figure 3-9 provides the initial, default screen, while Figure 3-6 shows the sample screen with the device paths filled in.

Figure 3-9 Initial Data Base Configuration Screen

Sybase can use either raw partitions or files for the data and log devices. The example provided in Figure 3-10 uses raw partitions for both the data and log devices. It also changes the sizes of each of these devices. Once filling in all the blanks, press the "next" button. At this point the information provided is validated and checks whether the Data Server "SYBASE" is running. If not, a warning message is presented, providing the procedure to bring it up. After successfully starting the server the process can continue.

Keymaster Database Configuration
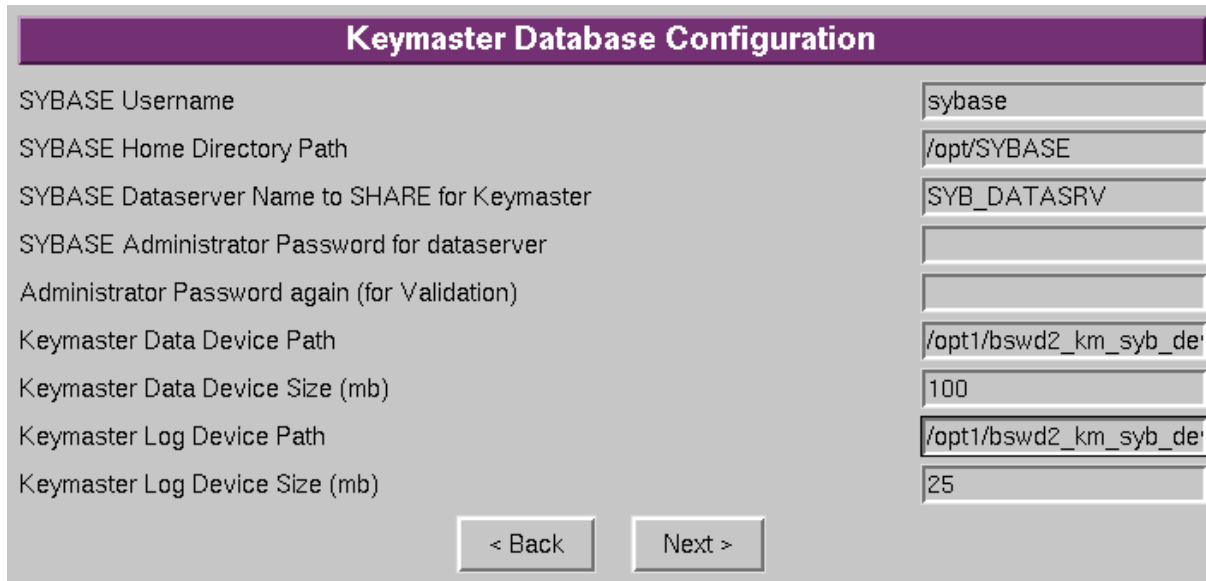
SYBASE Username	sybase
SYBASE Home Directory Path	/opt/SYBASE
SYBASE Dataserver Name to SHARE for Keymaster	SYB_DATASRV
SYBASE Administrator Password for dataserver	
Administrator Password again (for Validation)	
Keymaster Data Device Path	/opt1/bswd2_km_syb_dev
Keymaster Data Device Size (mb)	100
Keymaster Log Device Path	/opt1/bswd2_km_syb_dev
Keymaster Log Device Size (mb)	25

< Back   Next >

Figure 3-10 Example Data Base Configuration Screen

FIELDS VALIDATED	
Sybase Username	Username entered exists on system.
Sybase Home Directory Path	File <Path Entered>/bin/dataserver EXISTS.
Sybase Dataserver Name	Name entered is a currently defined dataserver (when in sharing mode). Also, when in sharing mode, verifies that dataserver entered is running.
Sybase Administrator Password	Installer enters it twice AND password is verified by doing test login into dataserver.
Data Device Path	Path EXISTS AND is writable by the Sybase User entered earlier AND there is enough space available for device (entered by installer).
Log Device Path	Path EXISTS AND is writable by the Sybase User entered earlier AND there is enough space available for device (entered by installer).

Table 3-4 Fields Validated

3.2.1.2 Keymaster Configuration

The next part of the installation process is to provide information necessary to configure the Keymaster.   This section provides the initial login (always 'bswduser') and password for the administrator to log into the interface and further configure the system. Figure 3-11 provides a sample of the Broadsword Keymaster Configuration Screen.

Figure 3-11 Broadsword Keymaster Configuration Screen
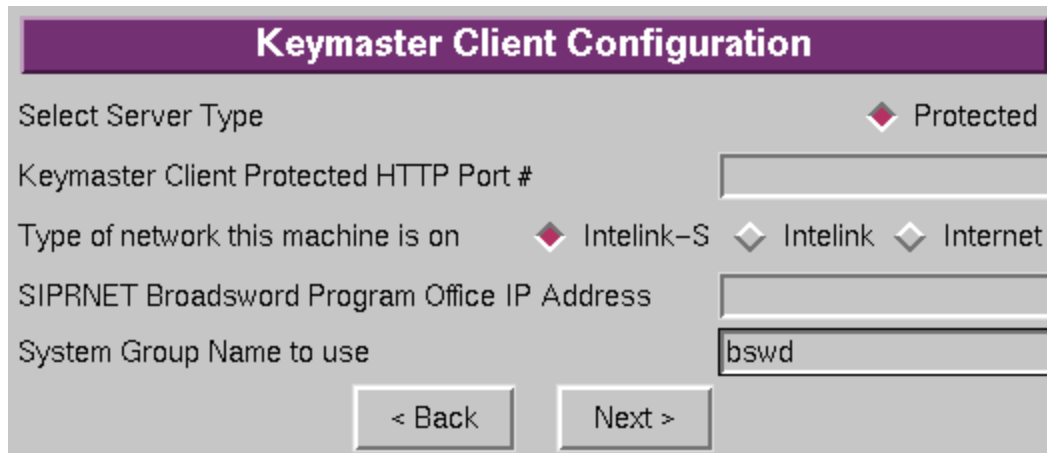
FIELDS VALIDATED	
'bswduser' Password	Installer enters it twice.

Table 3-5 Fields Validated

3.2.1.3 Client Configuration

After clicking on the "Next" button the configuration information is processed and validated. If successful, the installation process will continue with the configuration of the Keymaster Client. In this section, of the HTTPD ports, the network classification so that the appropriate Intelink Home Page URL is configured, the IP address of the Broadsword Program Office Home Page and the system group name. Figure 3-12 displays this page.

Figure 3-12 Keymaster Client Configuration Screen

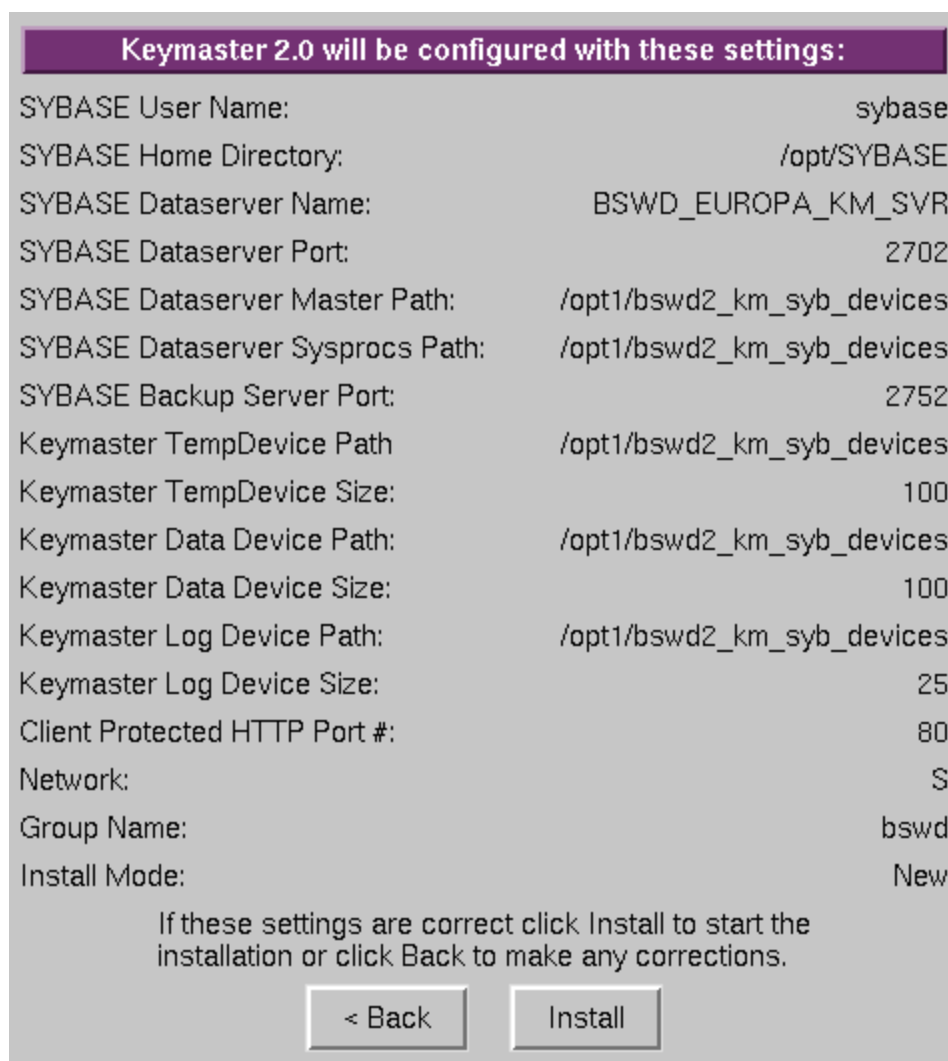| FIELDS VALIDATED	
Client Protected HTTP Port #	Port number is not already in use.
SIPRNET Broadsword Program Office IP Address	If Network Type selected is SIPRNET, this field cannot be empty.
System Group Name	Group name EXISTS on system.

Table 3-6 Fields Validated

The final portion of the installation process is to configure the Support Page. This page provides the necessary site's Points of Contacts (POCs) for Site Administration, ISSO and Intelink Site Manager. The System Administrator fields are mandatory. Figure 3-13 provides an example of the POC screen.

Figure 3-13 Point of Contact Information Screen

3.3   Confirming Installation Choices

Upon entering the POC information, the process continues by providing a screen, which displays the configuration information that has been entered thus far. At this point, clicking the "Install" button will continue the installation process. If changes are desired, use the "Back" button to proceed to the screen in which that item was configured. Figures 3-14 is an example of how a new data server confirmation screen will appear as and Figure 3-15 provide examples of what a shared data server screen will look like.

Keymaster 2.0 will be configured with these settings:	
SYBASE User Name:	sybase
SYBASE Home Directory:	/opt/SYBASE
SYBASE Dataserver Name:	BSWD_EUROPA_KM_SVR
SYBASE Dataserver Port:	2702
SYBASE Dataserver Master Path:	/opt1/bswd2_km_syb_devices
SYBASE Dataserver Sysprocs Path:	/opt1/bswd2_km_syb_devices
SYBASE Backup Server Port:	2752
Keymaster TempDevice Path	/opt1/bswd2_km_syb_devices
Keymaster TempDevice Size:	100
Keymaster Data Device Path:	/opt1/bswd2_km_syb_devices
Keymaster Data Device Size:	100
Keymaster Log Device Path:	/opt1/bswd2_km_syb_devices
Keymaster Log Device Size:	25
Client Protected HTTP Port #:	80
Network:	S
Group Name:	bswd
Install Mode:	New

If these settings are correct click Install to start the installation or click Back to make any corrections.

[< Back]   [Install]

Figure 3-14 Sample Based on New Data Server Confirmation Screen

Figure 3-15 Sample Based on Shared Data Server Confirmation Screen

3.4   Installation Progress
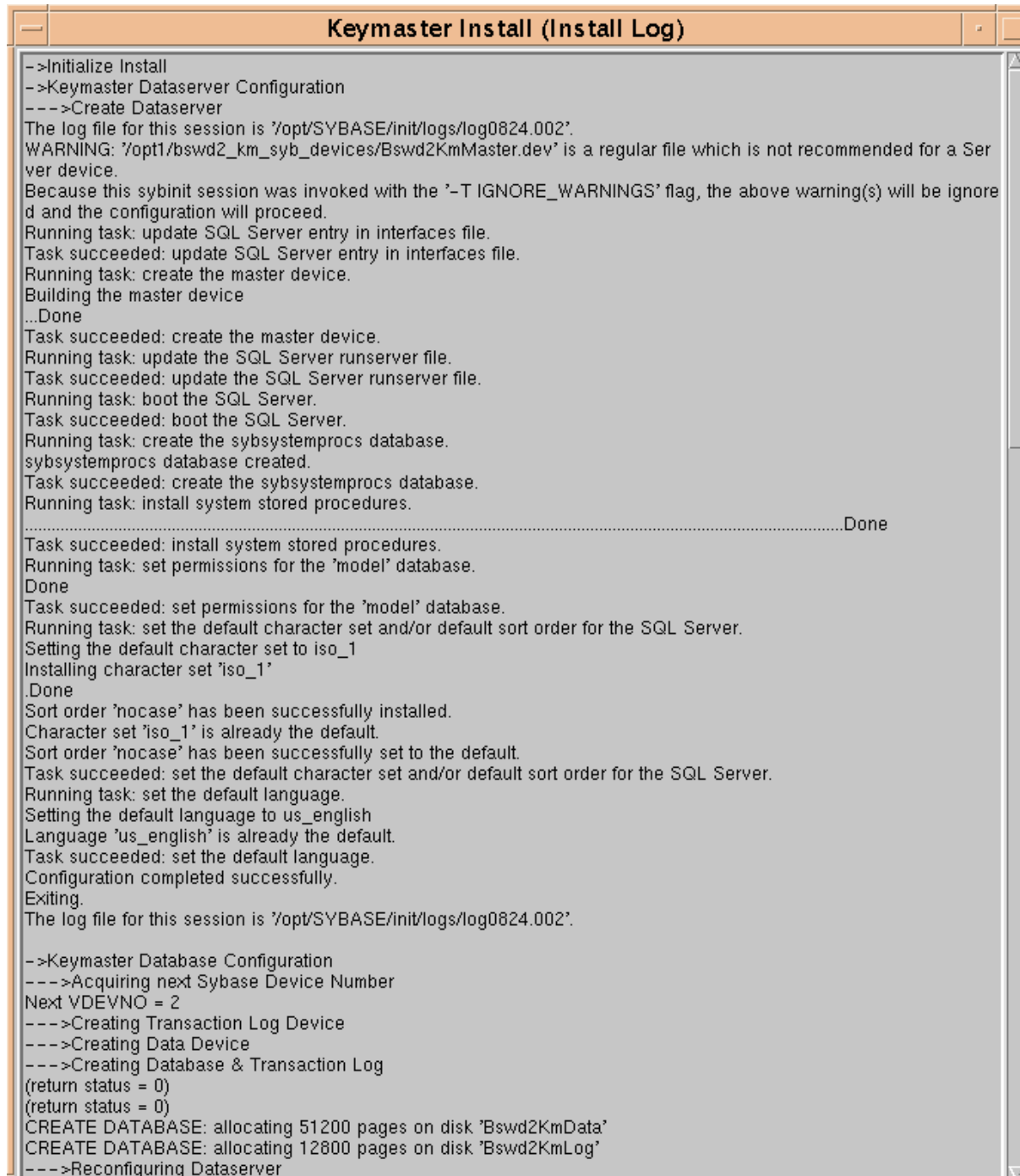
After clicking on the "Install" button, the installation process will continue to make the necessary changes. Two windows will appear to allow for monitoring of the progress. The first is a progress gauge, which provides for the percent of the total installation complete, while the second line indicates the percent complete of that specific part. Figure 3-16 provides an example of this screen.

Figure 3-16 Example of the Progress Gauge

The second screen provides a log of the process. Figure 3-17 provides a sample log screen. The information contained on the screen is also saved into a file for later reference. Also the configuration information is saved and if the installation process is restarted, it will read the saved file.

```
┌─┬──────────────────── Keymaster Install (Install Log) ──────────────┬─┬─┐
│─│                                                                    │▲│ │
│ │->Initialize Install                                                │ │ │
│ │->Keymaster Dataserver Configuration                                │ │ │
│ │--->Create Dataserver                                               │ │ │
│ │The log file for this session is '/opt/SYBASE/init/logs/log0824.002'.│ │ │
│ │WARNING: '/opt1/bswd2_km_syb_devices/Bswd2KmMaster.dev' is a regular file which is not recommended for a Ser│ │
│ │ver device.                                                         │ │ │
│ │Because this sybinit session was invoked with the '-T IGNORE_WARNINGS' flag, the above warning(s) will be ignore│ │
│ │d and the configuration will proceed.                               │ │ │
│ │Running task: update SQL Server entry in interfaces file.           │ │ │
│ │Task succeeded: update SQL Server entry in interfaces file.         │ │ │
│ │Running task: create the master device.                            │ │ │
│ │Building the master device                                          │ │ │
│ │...Done                                                             │ │ │
│ │Task succeeded: create the master device.                          │ │ │
│ │Running task: update the SQL Server runserver file.                 │ │ │
│ │Task succeeded: update the SQL Server runserver file.               │ │ │
│ │Running task: boot the SQL Server.                                  │ │ │
│ │Task succeeded: boot the SQL Server.                                │ │ │
│ │Running task: create the sybsystemprocs database.                   │ │ │
│ │sybsystemprocs database created.                                    │ │ │
│ │Task succeeded: create the sybsystemprocs database.                 │ │ │
│ │Running task: install system stored procedures.                     │ │ │
│ │...................................................................Done│ │
│ │Task succeeded: install system stored procedures.                   │ │ │
│ │Running task: set permissions for the 'model' database.             │ │ │
│ │Done                                                                │ │ │
│ │Task succeeded: set permissions for the 'model' database.           │ │ │
│ │Running task: set the default character set and/or default sort order for the SQL Server.│ │
│ │Setting the default character set to iso_1                          │ │ │
│ │Installing character set 'iso_1'                                    │ │ │
│ │.Done                                                               │ │ │
│ │Sort order 'nocase' has been successfully installed.                │ │ │
│ │Character set 'iso_1' is already the default.                       │ │ │
│ │Sort order 'nocase' has been successfully set to the default.       │ │ │
│ │Task succeeded: set the default character set and/or default sort order for the SQL Server.│ │
│ │Running task: set the default language.                             │ │ │
│ │Setting the default language to us_english                          │ │ │
│ │Language 'us_english' is already the default.                       │ │ │
│ │Task succeeded: set the default language.                           │ │ │
│ │Configuration completed successfully.                               │ │ │
│ │Exiting.                                                            │ │ │
│ │The log file for this session is '/opt/SYBASE/init/logs/log0824.002'.│ │ │
│ │                                                                    │ │ │
│ │->Keymaster Database Configuration                                  │ │ │
│ │--->Acquiring next Sybase Device Number                             │ │ │
│ │Next VDEVNO = 2                                                     │ │ │
│ │--->Creating Transaction Log Device                                 │ │ │
│ │--->Creating Data Device                                            │ │ │
│ │--->Creating Database & Transaction Log                             │ │ │
│ │(return status = 0)                                                 │ │ │
│ │(return status = 0)                                                 │ │ │
│ │CREATE DATABASE: allocating 51200 pages on disk 'Bswd2KmData'       │ │ │
│ │CREATE DATABASE: allocating 12800 pages on disk 'Bswd2KmLog'        │ │ │
│ │--->Reconfiguring Dataserver                                        │▼│ │
└─┴────────────────────────────────────────────────────────────────────┴─┴─┘
```

```
 Parameter Name              Default    Memory Used Config Value Run Value
 --------------------------- ---------- ----------- ----------- -----------
 total memory                  7500      15000       12288       7500
Configuration option changed. The SQL Server must be rebooted before the change
in effect since the option is static.

(return status = 0)
 Parameter Name              Default    Memory Used Config Value Run Value
 --------------------------- ---------- ----------- ----------- -----------
 number of user connections    25        1871        50          25
Configuration option changed. The SQL Server must be rebooted before the change
in effect since the option is static.

(return status = 0)
 Parameter Name              Default    Memory Used Config Value Run Value
 --------------------------- ---------- ----------- ----------- -----------
 number of devices             10        #4          20          10
Configuration option changed. The SQL Server must be rebooted before the change
in effect since the option is static.

(return status = 0)
 Parameter Name              Default    Memory Used Config Value Run Value
 --------------------------- ---------- ----------- ----------- -----------
 number of locks               5000      469         15000       5000
Configuration option changed. The SQL Server must be rebooted before the change
in effect since the option is static.

(return status = 0)
 Parameter Name              Default    Memory Used Config Value Run Value
 --------------------------- ---------- ----------- ----------- -----------
 procedure cache percent       20        960         25          20
Configuration option changed. The SQL Server must be rebooted before the change
in effect since the option is static.

(return status = 0)
Password correctly set.
Account unlocked.
New login created.
(return status = 0)
Database option 'trunc log on chkpt' turned ON for database 'bswd2_kmdb'.
Run the CHECKPOINT command in the database that was changed.
(return status = 0)
Database owner changed.
(return status = 0)
Adding server 'BSWD_EUROPA_KM_SVR', physical name 'BSWD_EUROPA_KM_SVR'
Server added.
(return status = 0)
--->Creating Temp Device
Extending database by 51200 pages on disk BswdTemp
Database option 'select into/bulkcopy' turned ON for database 'tempdb'.
Run the CHECKPOINT command in the database that was changed.
(return status = 0)
Database option 'trunc log on chkpt' turned ON for database 'tempdb'.
Run the CHECKPOINT command in the database that was changed.
```

```
(return status = 0)
--->Loading Schema
--->Loading Indexes
--->Loading Stored Procedures
->Configuring Keymaster Server
--->Updating Configuration Files
--->Encrypting Configuration Files
--->Generating Keymaster Digital Certificates
->Configuring Keymaster Client
--->Updating Configuration Files
--->Configuring Homepages
--->Configuring POC Page
--->Installing Initial Statistics Page
->Starting Keymaster Processes
--->


Default BSWD startup? (Y/N/Q) [Y]: You have chosen the following BSWD startup options:
    Start Sybase ................... Yes
    Start BSWD background APs........ Yes
    BSWD executables................ /opt/keymaster2.0/bin
Start these portions of BSWD? (Y/N/Q) [Y]: Starting Sybase...
SYBASE SQL Server is already running
SYBASE Backup Server is already running
Starting Background APs...
    Starting /opt/keymaster2.0/client/bin/KMserver
    Starting /opt/keymaster2.0/bin/keymaster.SVR4
    Starting /opt/keymaster2.0/bin/jivacron
    Starting /opt/keymaster2.0/bin/remote_plugin.SVR4

Keymaster 2.0 Process Status (Tue Aug 24 10:40:59 EDT 1999):

running     /opt/keymaster2.0/bin/keymaster.SVR4
running     /opt/keymaster2.0/bin/jivacron
running     /opt/keymaster2.0/bin/remote_plugin.SVR4
running     /opt/keymaster2.0/client/bin/KMserver

->Cleaning up
->Done
--->Done
```

Figure 3-17 Sample Log Screen

If the installation is successful, the last screen displayed will be the "Installation Complete" screen (as shown in Figure 3-18).
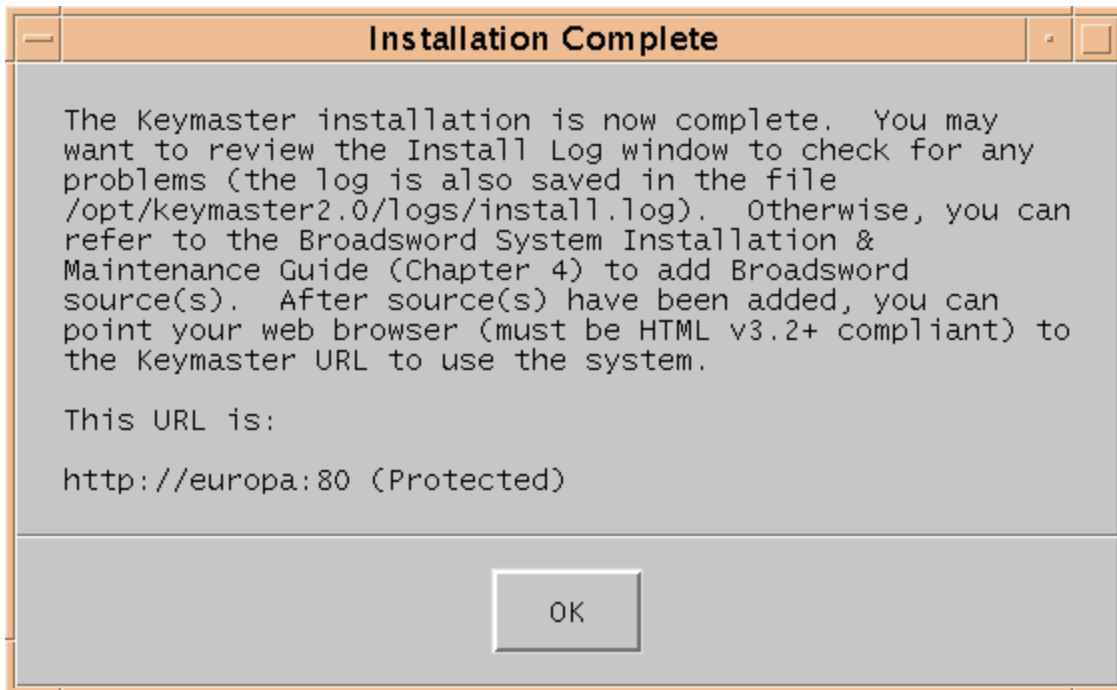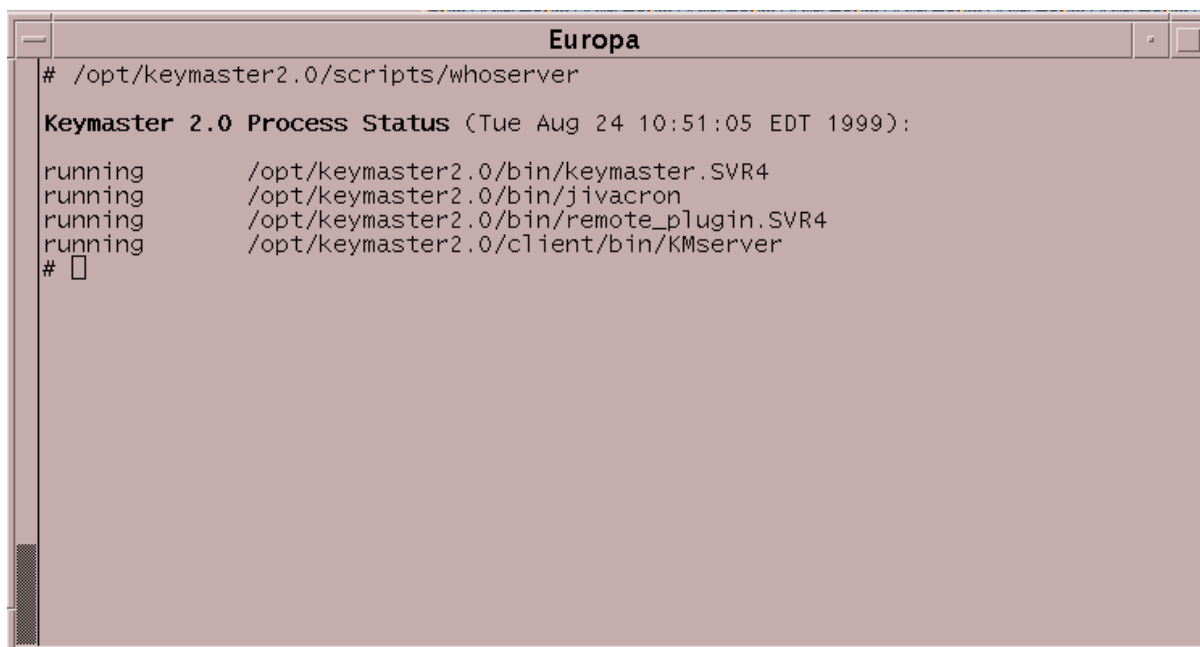
Figure 3-18 Installation Complete

3.5   Installation Verification

At this point the installation process is complete.   To verify the installation has completed correctly, the following command may be executed:

/opt/keymaster2.0/scripts/whoserver

If all processes are shown to be running, the installation most likely has succeeded. Figure 3-19 provides a sample listing of the processes that should be running. If for some reason one or a number of the processes are not running, check the log window (or the log file) for any obvious problems during the installation. If the problem cannot be fixed at this point contact the Broadsword help desk, otherwise continue to Chapter 4 – Server Configuration.

```
Europa
# /opt/keymaster2.0/scripts/whoserver

Keymaster 2.0 Process Status (Tue Aug 24 10:51:05 EDT 1999):

running         /opt/keymaster2.0/bin/keymaster.SVR4
running         /opt/keymaster2.0/bin/jivacron
running         /opt/keymaster2.0/bin/remote_plugin.SVR4
running         /opt/keymaster2.0/client/bin/KMserver
#
```

Figure 3-19 Sample Listing of Processes Running

In addition, the system administrator may reference the ***Version Description Document (VDD)*** for a complete listing of files installed, along with appropriate path and permissions information.

3.6 Uninstalling the System

There are many possible reasons for uninstalling the system. These reasons could range from the fact that something went wrong with the installation process and there is a desire to start from the beginning again, or another possible reason is that you wish to remove the previous version. This section is divided into two parts: (1) removing a previous version and (2) removing the current version.

3.6.1 Removing a Previous Version
To remove a previous version of Keymaster, you must shutdown any Keymaster processes, remove all Keymaster files, and drop the Keymaster database and/or dataserver. (currently not available)

3.6.2   Removing the Current Version

To remove the current version of the Keymaster, you must shutdown any Keymaster processes, remove all Keymaster files, and drop the Keymaster database and/or dataserver.

1 **Stopping the System Processes**

To stop all the necessary processes (must be done as user root):

> ***/opt/keymaster2.0/scripts/stopserver <cr>***

IMPORTANT NOTE: Before doing the procedures below, make sure to backup your system.

2 **Dropping the Data Base**

To drop the database, do the following as your sybase user (**NOTE: this is only an example – your situation may differ**):

su – <sybase user> <cr>
/bin/csh <cr>
setenv SYBASE <keymaster Sybase Home Dir> <cr>
setenv DSQUERY <keymaster Sybase Server Name> <cr>
${SYBASE}/bin/isql –Usa –P<Sybase sa Passwd> -y${SYBASE}<cr>
1> select name, phyname from sysdevices <cr>
2> where name = "Bswd2KmData" <cr>
3> or name = "Bswd2KmLog" <cr>
4> go <cr>

name
      phyname

Bswd2KmData
      /dev/rdsk/c0t5d0s7
Bswd2KmLog   **(Make note of these values)**
      /dev/rdsk/c0t4d0s6

(2 rows affected)

1> drop database bswd2_kmdb <cr>
2> go <cr>
1> sp_dropdevice Bswd2KmLog <cr>
2> go <cr>
Device dropped.
(return status = 0)
1> sp_dropdevice Bswd2KmLog <cr>
2> go <cr>
Device dropped.
(return status = 0)
1> shutdown with nowait <cr>
2> go <cr>
Server SHUTDOWN by request.
The SQL Server is terminating this process.
00:98/06/08 15:39:15.94 server SQL Server shutdown by request.
00:98/06/08 15:39:15.98 kernel ueshutdown: exiting
DB-LIBRARY error:
    Unexpected EOF from SQL Server.

If above phyname fields begin with /dev, **do not perform any remove commands**. Otherwise, remove both of the phyname paths noted above:

> *rm* < Bswd2KmData phyname> ***<cr>***
> *rm* < Bswd2KmLog phyname> ***<cr>***

If Keymaster is sharing another Sybase Dataserver, **do not perform any further action**. You must proceed to step 3 below. Otherwise, to remove the **Keymaster Dataserver**, perform the following:

> If Dataserver Master, Sysprocs, and TempDevice Paths (Worksheet #10, 11, 14) begin with /dev, **do not perform any remove commands**. Otherwise, remove all of these device files, substituting the appropriate paths in <> with your actual paths:

> > *rm /*<Worksheet #8 Path>*/Bswd2KmMaster.dev <cr>*
> > *rm /*<Worksheet #9 Path>*/Bswd2KmSysProcs.dev <cr>*
> > *rm /*<Worksheet #12 Path>*/Bswd2KmTemp.dev <cr>*

> Perform one of the following to remove the Keymaster Sybase server from the Sybase interfaces file:

For SQL Server:

(Important: Only delete a newly created Keymaster dataserver, not one that is shared with another application!!)

> *${SYBASE}/install/sybinit <cr>*

and enter the following input:

INPUT	DESCRIPTION OF ACTION
1 *<cr>*	{Specify Release Directory}
Sybase Home Dir	{Worksheet #7} <cr>
2 *<cr>*	{Edit Interfaces File}
4 *<cr>*	{Delete an existing entry}
Choose # for Keymaster Server	{Worksheet #8} <cr>
y <cr>	{Remove entry}
y <cr>	{Write changes}
CTRL-A CTRL-A	{Exit sybinit}

For Adaptive Server:

(Important: Only delete a newly created Keymaster dataserver, not one that is shared with another application!!)

> *setenv DISPLAY* <current X display>

> *${SYBASE}/bin/dsedit <cr>*

Make sure "Sybase Interfaces File" is highlighted and click "OK".

Select the Keymaster server entry from the available servers list and click "Delete server entry".

Click "Yes" to confirm deletion. The Keymaster dataserver will disappear from the available servers' list.

Click "Close session"
Click "Exit"
Click "Yes" to confirm exit

3 Removal of Keymaster Software

The final step is to remove the software installed as part of the Keymaster installation:

> *cd /opt/keymaster2.0 <cr>*
> */bin/rm –rf * <cr>*

CONFIGURATION

The purpose of this part is to provide detailed information to configure the system and tailor the system to the site's requirements.

Topics covered in this part:

System Configuration
Editing/Modifying Keymaster Parameters

User Maintenance
Editing/Modifying User Privileges

Client Requirements
HTML Browsers

Chapter 4
System Configuration

Once the installation of the basic system is done, site specific configuration must be performed. This chapter provides details on how to add local sources, modify system and gatekeeper parameters, register the gatekeeper with others, setting up access to remote sources and tailoring data element values. By clicking on the System Config line (under the Administration function off the side bar), the Administrator is presented with a series of tabs as shown in Figure 4-1.
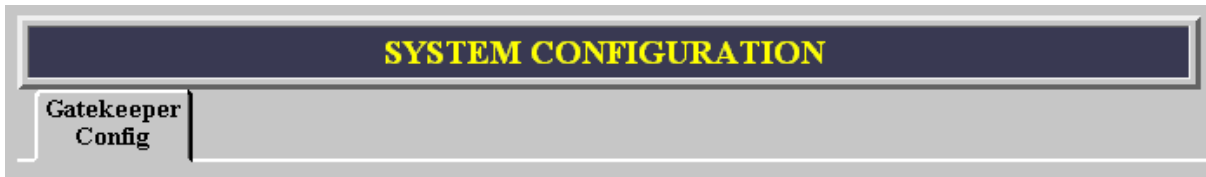

Figure 4-1 System Configuration Tools

4.1 Gatekeeper Configuration

The "Gatekeeper Config" screen allows the administrator to modify various parameters of the local Gatekeeper. Figure 4-2 presents a sample "Gatekeeper Config" screen.

Figure 4-2 Sample "Keymaster Config" Screen

Several configuration items, their current (editable) values, and help text for each are presented. Select the field(s) of the items that require modification, enter their new value, and when complete, hit the "**Save**" button. You may hit "**Reset**" to revert any changes you have been making to the page and start over.
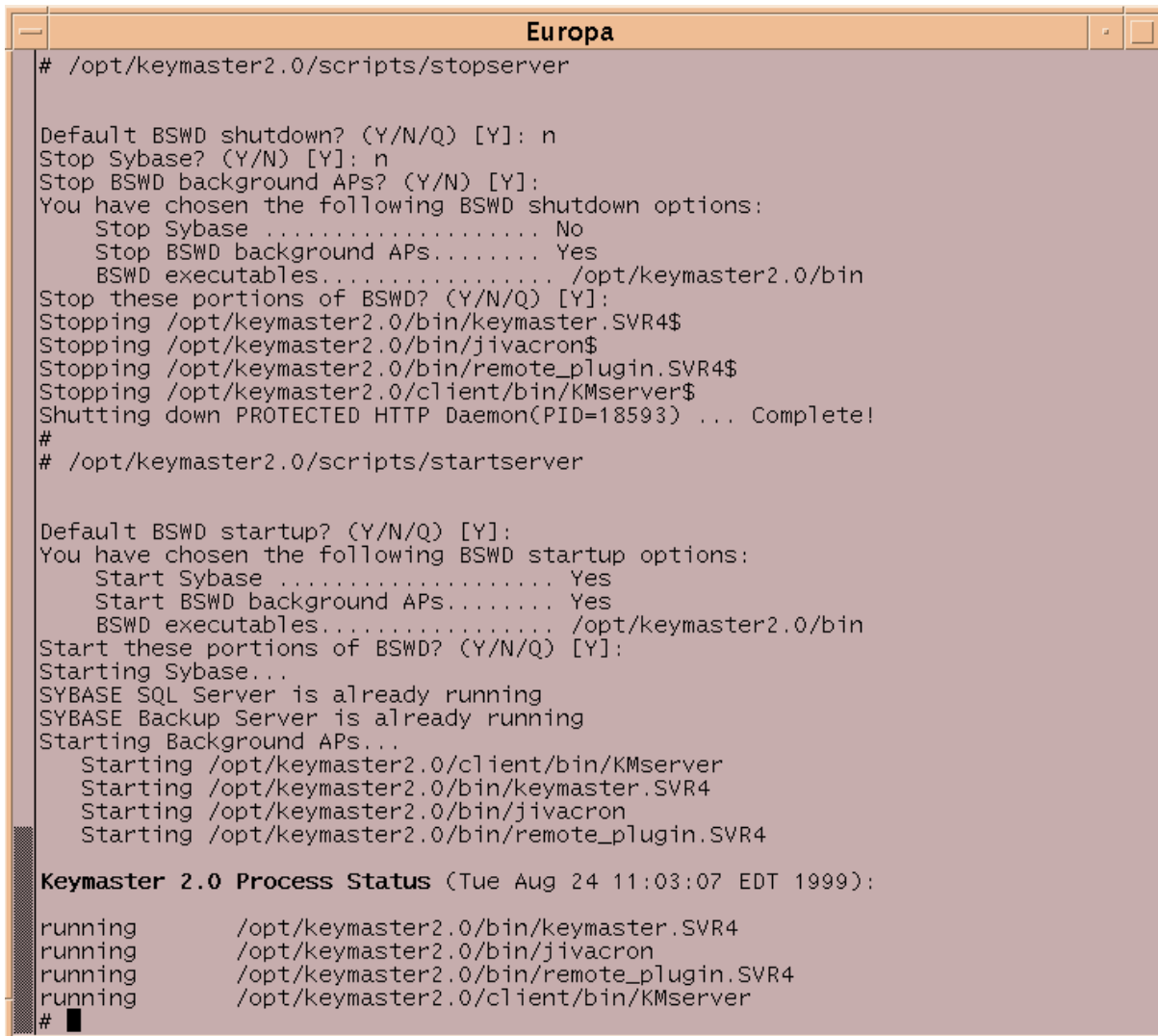
> **Note:** After applying a change to the "Client Idle Timeout", Keymaster Server must be restarted to force it to reread the configuration file. To restart the Keymaster process perform the following as user root:

/opt/keymaster2.0.scripts/stopserver   (only stops keymaster, background apps)

/opt/keymaster2.0/scripts/startserver   (accept all defaults)

The screen below illustrates an example of this:

```
┌─────────────────────────────── Europa ──────────────────────────────┐
│ # /opt/keymaster2.0/scripts/stopserver                                │
│                                                                       │
│                                                                       │
│ Default BSWD shutdown? (Y/N/Q) [Y]: n                                 │
│ Stop Sybase? (Y/N) [Y]: n                                             │
│ Stop BSWD background APs? (Y/N) [Y]:                                   │
│ You have chosen the following BSWD shutdown options:                  │
│     Stop Sybase ...................  No                                │
│     Stop BSWD background APs........ Yes                               │
│     BSWD executables................ /opt/keymaster2.0/bin            │
│ Stop these portions of BSWD? (Y/N/Q) [Y]:                             │
│ Stopping /opt/keymaster2.0/bin/keymaster.SVR4$                        │
│ Stopping /opt/keymaster2.0/bin/jivacron$                              │
│ Stopping /opt/keymaster2.0/bin/remote_plugin.SVR4$                    │
│ Stopping /opt/keymaster2.0/client/bin/KMserver$                       │
│ Shutting down PROTECTED HTTP Daemon(PID=18593) ... Complete!          │
│ #                                                                     │
│ # /opt/keymaster2.0/scripts/startserver                               │
│                                                                       │
│                                                                       │
│ Default BSWD startup? (Y/N/Q) [Y]:                                    │
│ You have chosen the following BSWD startup options:                   │
│     Start Sybase ...................  Yes                              │
│     Start BSWD background APs........ Yes                              │
│     BSWD executables................ /opt/keymaster2.0/bin            │
│ Start these portions of BSWD? (Y/N/Q) [Y]:                            │
│ Starting Sybase...                                                    │
│ SYBASE SQL Server is already running                                  │
│ SYBASE Backup Server is already running                               │
│ Starting Background APs...                                            │
│    Starting /opt/keymaster2.0/client/bin/KMserver                     │
│    Starting /opt/keymaster2.0/bin/keymaster.SVR4                      │
│    Starting /opt/keymaster2.0/bin/jivacron                            │
│    Starting /opt/keymaster2.0/bin/remote_plugin.SVR4                  │
│                                                                       │
│ Keymaster 2.0 Process Status (Tue Aug 24 11:03:07 EDT 1999):          │
│                                                                       │
│ running      /opt/keymaster2.0/bin/keymaster.SVR4                     │
│ running      /opt/keymaster2.0/bin/jivacron                           │
│ running      /opt/keymaster2.0/bin/remote_plugin.SVR4                 │
│ running      /opt/keymaster2.0/client/bin/KMserver                    │
│ # █                                                                   │
└───────────────────────────────────────────────────────────────────────┘
```

Figure 4-3 Sample Screen of Restarting Keymaster

4.2 Gatekeeper Registration

The purpose of this section is to allow the Keymaster to register new Gatekeepers through the use of digital certificates.

4.2.1 How to Register a New Gatekeeper

1. The POC for the new gatekeeper will contact the Keymaster via telephone and request to register their gatekeeper.

2. The Keymaster will click the **Init Registration** button to generate the one time password used for the registration process.

3. The Keymaster will then transmit via secure means, the Keymaster's IP address, port number, and the one-time password for the POC of the gatekeeper.

4. The POC of the gatekeeper will then use the **Administration -> System Configuration -> Register** Gatekeeper page to enter the required data and complete the registration process.

5. After the registration process has been initiated by the Keymaster, that status of the registration process will be updated and displayed every minute until the registration process is completed or terminated.

6. The Keymaster may click on the **Abort Registration** button to abort the current registration process anytime during the registration process.

Note: Only one registration process may be initiated and active at any given time.
Clicking on any link on the navigation bar during the registration process will terminate the registration process.

Figure 4-4 is a sample screen of the start registration function.

Figure 4-4 Start Registration

4.3 Viewing and UnRegistering Gatekeepers

The purpose of this section is to allow the Keymaster to view all registered gatekeepers and to un-register any or all gatekeepers. Each registered gatekeeper has the POC information and all of its backside sources listed.

4.3.1 How to Un-Register a Gatekeeper

1. Click on the box next to the desired Gatekeeper in the Un-Register column.

2. Click on the button at the bottom of the page to submit the changes.

Note: Notice under each gatekeeper in the right column are the sources that are available to that particular gatekeeper. Keymaster users can only un-register the gatekeeper as a whole and not the individual sources.

Figure 4-5 is a sample screen of the viewing/un-registering of gatekeepers

UnRegister	GATEKEEPER	SOURCE
☐	beth Gatekeeper	**POC:**
		IPA 1.2.3 at Moon via Beth
		IPL 1.0 at Atlas via Beth
		IPL 2.1 at Titania via Beth
		5D at Venus via Beth
		AMHS at Elara via Beth
		CSIL at Neptune via Beth
		IESS w/IDEX at IESS0 via Beth
		MIDB at Hoth via Beth
		NDS at Moon via Beth
		AODB at Juliet via Beth
☐	daleth Gatekeeper	**POC:**
		IPL 1.0 at Sun via Daleth
		AMHS at Elara via Daleth
		IESS at IESS0 via Daleth
		MIDB at Hoth via Daleth

Figure 4-5 View/Remove Gatekeepers
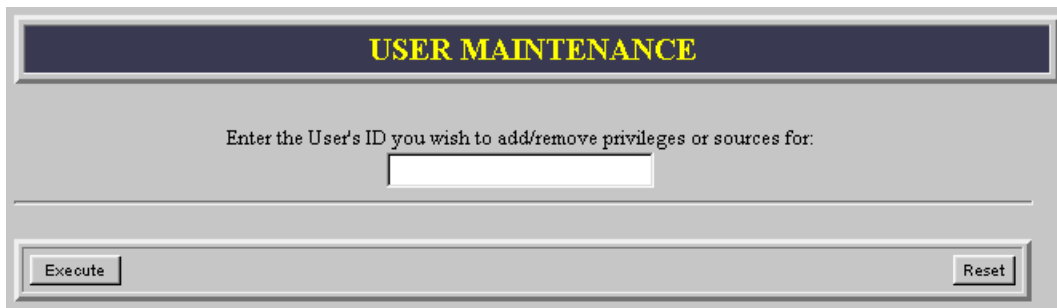
Chapter 5
User Maintenance

The purpose of the "User Maintenance" screen is to allow the administrator to add/remove a given user to/from having access to certain privileges and available sources. After clicking on "User Maintenance" under the Administration section, the User Maintenance screen will appear as shown in Figure 5-1.

Figure 5-1 Sample "User Maintenance" Screen

After entering a legitimate (i.e., existing) user id, a list of available privileges that are accessible for the site will be provided. This form will be pre-filled with those privileges that are currently assigned to that user id. Figure 5-2 provides an example screen for the user id, "bswduser".

The "**USER ACCESS**" section displays a list of the accessible privileges, indicating whether the given user is currently allowed to access each of them, check boxes allowing the means to change each access setting.

IMPORTANT NOTE: "**USER ACCESS**" and "**ACCESS**" listings that show "Add Access" checkboxes are displayed in red.

By clicking on the "Execute" button, any changes made to the user's privileges will be processed. Clicking on the "Reset" button will return the values to those that previously existed.
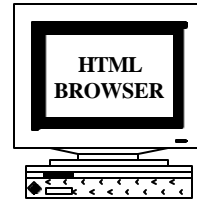
After executing a change in USER ACCESS, the affected user will not see these new accesses will not see these new accesses until the next time they log into the system.

Figure 5-2 Setting User Privileges

HTML
BROWSER

Chapter 6
Client Requirements

The purpose of this chapter is to identify what software or application(s) that will be required to access the system. As a minimum, an HTML browser will be necessary. There is NO specific client software required to be loaded. Specific topics to be covered include:

- HTML Browsers

6.1 HTML Browsers

Keymaster requires a web browser which supports the HTML 3.2 standard (i.e.- is frames enabled). Netscape 3.0x or Internet Explorer 3.0x are recommended as a minimum. The system DOES NOT use either JAVA or Javascript and hence JAVA and Javascript options need not be set. The interface is best viewed using Netscape 4.0x or Internet Explorer 4.0x.

When using Internet Explorer 3.x, the cursor does not change when a new page is loading. The only way to see if a new page is loading after clicking on a link or button is to leave the cursor over it.

If caching is enabled on either Internet Explorer or Netscape, it is possible to visit previously loaded pages without reloading them from the server on which they reside. If there are any form elements on these pages, all data previously entered will still be present. Thus it would be possible to complete a Broadsword session, and then return to the login page and connect without retyping one's password. This problem may be circumvented by making sure to exit the browser after logging out, or by clearing the cache after a session. Another option is disabling the cache (see Note below).

When using Netscape, resizing the browser window may cause the current page's data to be lost. The server will respond with a missing form data error. Reloading he form data will not return you to the expected page, since all of Broadsword's pages are created dynamically. In order to solve this problem, the user must enable the memory or disk cache under advanced preferences. This value should be suitably large (1000 K should work).

Operating System	Browser
Solaris 2.5.1	Netscape v3.01, 4.02, 4.05
Windows 95/NT v4.0	Netscape v3.01, 4.01, Internet Explorer 3.01, 4.01

Table 6-1 Summary of Supported HTML Browsers

Project Broadsword has the ability to access virtually any type of product. Some product formats included are TIFF, NITF 1.1, NITF 2.0, MPEG, and Quicktime, to name a few. However, a Browser inherently supports none of these formats. Helper applications, also called external viewers, are software programs external to the Web browser that are used to open files of data types that the browser doesn't natively recognize.

The majority of these helper applications have setup utilities, which automatically make the browser aware of their existence on PC and Macintosh platforms. However in some cases the user can configure the browser manually to make them aware of helper applications. Some examples of valid configurations are available on the Helper Configuration page.

IMPORTANT NOTE: Because of how fast Browsers are being released today, it's extremely difficult to keep up configuration issues. Please refer to the applicable browser documentation for configuration information. Click on the links below to view a listing of the helper applications or viewers that can be launched from a browser for different file formats.

PART III

MAINTENANCE

The purpose of this part is to provide detailed information to maintain the system.

Topics covered in this part:

System Status
> Daemon Status
> Starting/Stopping the System Processes
> Queue Maintenance
> Set Debug Flags
> System and Log Information

Chapter 7
System Status

System Status provides the administrator the ability to manage the operations of the system. Tools are provided to show if all the necessary processes are running, the status of the message queues used for communication between the processes, management of the logs used by the system and available system space and the ability to turn on/off debug flags to assist in identifying problems. By clicking on the System Status line (under the Administration function off the side bar), the Administrator is presented with a series of tabs as shown in Figure 7- 1.

Figure 7-1 System Status Tools

7.1 Daemon Status

The "Daemon Status" screen provides the administrator with the status of the processes that are required to run the current system, identifies possible problems and suggests solutions to these problems.   Figure 7-2 provides a sample of the Daemon Status screen.
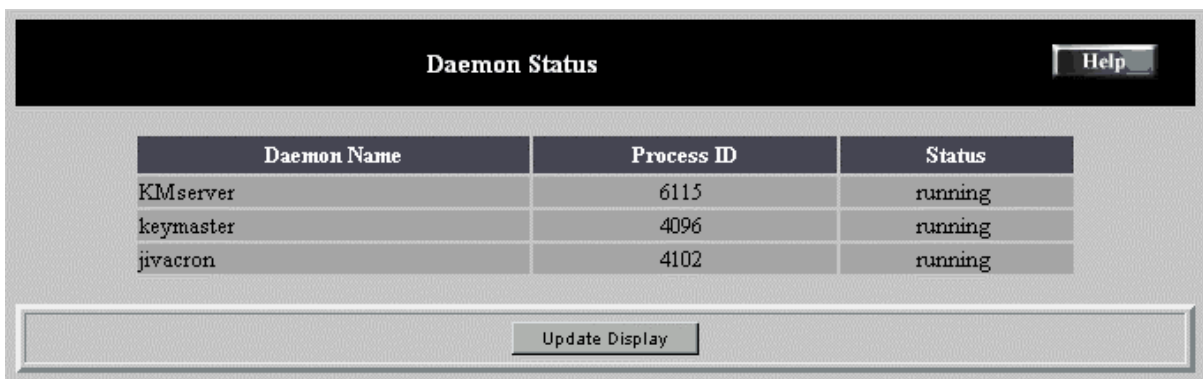

Figure 7-2 Sample "Daemon Status" Screen

The "**Daemon Status** " screen contains a table that shows the **Daemon Description**, **Process ID** and **Status** for each process. A description of each column follows:

Column Name	Contents
Daemon Name	Name of the daemon process. MANDATORY PROCESSES INCLUDE: keymaster, KMserver, jivacron, remote_plugin,
Process ID	Process ID of the corresponding daemon process. POSSIBLE ENTRIES: Integer value, n/a
Status	Status of the corresponding daemon process. POSSIBLE ENTRIES: running, not running, started, unable to start, stopped, unable to stop

Table 7-1 Summary of Values

Upon installation, only the mandatory processes (keymaster, KMserver, jivacron, remote_plugin), will appear in the process table. Each process will have a process id of **n/a** and a status of **not running**.

It is not the purpose of this screen to start/stop the processes. It is not possible to provide this capability through the interface since two out of the three mandatory processes must be running for the interface to work. Thus, it would be possible to stop all processes through the interface, but not be able to start them (or even do anything else). Scripts are provided for the administrator to start, stop and find out whether system processes are running. These scripts are run from the command line.

There is only one button on this page: "**Update Display**". Clicking the "Update Display" button on the bottom button bar updates the entries in the process table, showing the current state of each process.

To Start the System

To **start** the all processes, do the following:

> *cd /opt/keymaster2.0/scripts<cr>*
> *./startserver<cr>*

and press *<cr>* to take the defaults to startup all processes.

To Stop the System

To **stop** all processes, do the following:

> *cd /opt/keymaster2.0/scripts<cr>*
> *./stopserver<cr>*

and press *<cr>* to take the defaults to startup all processes**.**

To Check the System

Also provided is a command line script which checks the status of the processes without having to log into the interface.

To **check** all processes, do the following:

cd /opt/keymaster1.0/scripts<cr>
./whoserver<cr>

7.1.1 Possible Problems/Solutions

The process table should contain information on each of the mandatory processes. Also, any local plugins should also appear in the process table, if the administrator configured them. There are several problem conditions that may occur. The following table lists these conditions. For each problem condition the normal process id and status is shown, along with the process id and status that appears when there is a problem. A possible solution to the problem is also provided.

Note: The Daemon Description, Process ID and Status will appear in red when a status of "**unable to start**" or "**unable to stop**" is displayed.

Condition	Normal		Problem		Possible Problem Solution
	Process ID	Status	Process ID	Status	
Process Should Be Running	integer value	running	n/a	not running	Check for existence of the Daemon Description file (binary). If binary exists, check its ownership and permissions. Also, check for a core file to determine if the process died.
Local Plugin does not Appear	-	-	-	-	Local plugin was not installed. Follow the instructions under Upon Installation to install the plugin.
Mandatory Process does not Appear	-	-	-	-	Contact Technical Assistance, which is identified on the Support screen.

Table 7-2 Summary of Potential Problems/Solutions

7.2 Queue Maintenance

The "Queue Maintenance" screen allows the administrator to perform periodic maintenance on or trouble shoot problems related to the state of the message queue. The message queue shows the

message traffic that occurs between the session manager (KMserver) and client processes (cgi-bins). Figure 7-3 provides a sample of the Queue Maintenance screen.

Figure 7-3 Sample "Queue Maintenance" Screen

The "**Queue Maintenance**" screen contains a table that displays information about the current state of the message queue. A description of the information in this table follows:

Column Name	Contents
Queue ID	Identifier for the message queue. VALID VALUE: integer
Access Modes	Message queue access modes are nine characters interpreted as three sets of three bits each. Reading from left to right, the first set refers to the owner's permissions; the next to permissions of others in the user group of the message queue; and the last to all others. Within each set, the first character indicates permission to read, the second character indicates permission to write or alter the message queue, and the last character is currently unused. The permissions are indicated as follows: r Read permission is granted; w Write permission is granted; a Alter permission is granted; - The indicated permission is not granted. VALID VALUE: rw-rw-rw-
Owner	Login name of the owner of the message queue. VALID VALUE: root
Current Bytes*	Number of bytes in messages currently outstanding on the message queue. VALID VALUE: less than the value of **Max Bytes**
Current # of Messages *	Number of messages currently outstanding on the message queue. VALID VALUE: any number that allows the **Current Bytes** for these messages to not exceed **Max Bytes**
Max Bytes	Maximum number of bytes allowed in messages outstanding on the message queue. VALID VALUE: integer
Last Pid to Send	Process ID of the last process to send a message to the queue. VALID VALUE: integer
Last Pid to Receive	Process ID of the last process to receive a message from the queue. VALID VALUE: integer

Table 7-3 Summary of Queue Maintenance Values

Note: Current Bytes and Current # of Messages will appear in red when the Current # of Messages is greater than zero.

There are two buttons located on the bottom of the page: (1) **"Update Display"** and (2) **"Pop Message".** The "Update Display" button allows the administrator to update the message queue table to display the latest information about the queue. Since the table represents a snapshot in time and

does not automatically update itself, it is necessary to initiate the update. This is done by clicking the "Update Display" button. There are times when a message can get stuck in the queue. This can cause either an increase in response time or no response at all. Clicking on the "Pop Message" button allows the administrator to remove a message from the queue. Each click of the button will remove the message that is at the top of the queue.

7.2.1 Possible Problems/Solutions

Problems that may be related to the state of the message queue and possible solutions to these problems are listed in the following table:

Problem Condition	Possible Solution
A user cannot log into Keymaster or logins are taking an unusually long time	If the administrator cannot log into Keymaster the session manager, KMserver, may not be running. At the unix level check to see if the process KMserver is running. If KMserver is **not** running, start it up by typing /opt/bswd<version_number/bin/startKMserver. If KMserver is running, follow the instructions in the next problem solution.
Response time is unusually long after clicking any action button - OR - Get no response after clicking any action button	Messages may be stuck on the message queue or the **Current Bytes** on the queue may have exceeded the **Max Bytes.** Check for this by clicking the "**Update Display**" button. If the **Current Bytes** and **Current # of Messages** are greater than zero and these entries don't go down after clicking the "**Update Display**" button several times, waiting a few seconds between tries, then messages are stuck on the queue. Release stuck messages from the queue by clicking the "**Pop Message**" button (see the "Button Functions" section for a description). Upon clicking the "**Pop Message**" button, information on the message that was removed from the queue will appear in a table (see the "Pop Message Info" section). Try popping all the stuck messages from the queue and see if the problem goes away. If the problem remains contact Technical Assistance, which is identified on the "Support" screen, and refer to the "**Pop Message Info"** table when discussing the problem.

Table 7-4 Summary of Potential Problems/Solutions

7.2.2 Pop Message Info

The "**Pop Message Info"** table contains three types of information on the message that was popped from the message queue after clicking the "**Pop Message**" button. A description of these information types follow.

Information Type	Description
Receiving Process: OR **Pid of Receiving Process:**	Identifies the process that was to receive the message appearing in the queue. VALID VALUES: conan for **Receiving Process**, process id of client process for **Pid of Receiving Process**
Command:	The command that initiated the message that was put on the queue by the sending process. VALID VALUES (conan): Server Response, Server Administration VALID VALUES (client processes): User Login, Save Data Set, Retrieve Data Set, Save User Record to File, Retrieve User Record, Update User Record, User Logout, Make Query, Update User's Preferences, Pull Product, Update E-mail Notification Profiles, Remove Data Set, Update Data Set, E-mail Notification Query, Update Map Data, Failed Login, Message Queue Initialization Failed, Send Message Failed, Receive Message Failed, No Login, User's Session Folder not

	Found, User's Preferences Folder not Found, User Record not Found, User's Preferences data not Found, Bad Query Status, Unknown Command
Message:	The message that was put on the queue by the sending process. If the sending process was conan, the message is the outcome of a request performed by conan. If the sending process was a client process, the message is information needed by conan to perform a request of the client process.

Table 7-5 Summary of Messages

7.3 Set Debug Flags

The "Set Debug Flags" screen allows the administrator to set or clear debug flags prior to viewing a log file. The "**Set Debug Flags** " screen should be used when debugging a problem with the assistance of a technical support person. (Technical Assistance is identified on the **Support** screen.) Technical Assistance would instruct the administrator to set certain debug flags depending on the problem being addressed. The information sent to the log file depends on what debug flags are set. Figure 7-4 provides a sample of the Set Debug Flags screen.

Figure 7-4 Sample "Set Debug Flags" Screen

The "**Set Debug Flags**" screen contains a table with two columns. These columns are described as follows:

Column Name	Contents
Debug	Checkbox for selecting the debug flag.
Flag Name	Name of debug flag. AVAILABLE FLAGS: Server, Configuration, Automatic Logout, Session Manager, Communication, BQS, Hit List, Clean Up, EMN, Registered, Cart

Table 7-6 Summary of Values

There a four buttons available on this page: (1) "**Apply Changes**", (2) "**Toggle All On**", (3) **"Toggle All Off**", and (4) "**Reset**". Clicking on the "Toggle All On" button will turn on all the available flags while clicking on the "Toggle All Off" button will turn off all the flags. To select one or a subset of the available flags, click inside the box located next to the item and click on the "Apply Changes" button. The "Reset" button will reset the form to those items that were check upon entering the page.

The log file can be viewed by clicking on the anchor titled "View Conan Log File" located just above the button bar.

7.4 System and Log Information

The "System and Log Information" screen allows the administrator to monitor and/or free up disk space due to log files that are used by the system. Through the "**System and Log Info**" screen the administrator can select log files to be purged and monitor disk usage information on the file system where the system resides.   Figure 7-7 provides a sample of the "System and Log Info" screen.

Figure 7-7 Sample "System and Log Info" Screen

The "**System and Log Info**" screen contains two sections. The top section contains the log file information while the bottom section contains the disk usage information. The administrator should use the information from these two sections to determine if it is necessary to free up disk space due to the log files. The log file information is presented in a table with three columns which are described as follows:

Column Name	Contents
Select	Checkbox for selecting the log file.
Log File	Name of log file. ACCESSIBLE LOG FILES: error_P.log, access_P.log, jivacronlog
Size in Bytes	Size of the log file.

Table 7-7 Summary of Values

The purpose of the accessible log files are described as follows:

Log File	Purpose
error_P.log	Logs httpd error information.
access_P.log	Logs httpd activity information.
agent_log	Logs browser identification information.
refer_log	Logs browser URL/page information.
conan.log	Logs session and client activity information.

Table 7-8   Summary of Log Files

Note: There may be additional Log Files that appear in this screen.

There are two buttons on this page: **(1) "Update Display" and (2) "Purge Log File".** The "Update Display" button allows the administrator to display the latest information about the sizes of the log files. Since the table represents a snapshot in time and does not automatically update itself, it is necessary to initiate the update. This is done by clicking the "Update Display" button. To remove or purge the log files, the administrator must identify the file by clicking in the box next to the log file name and pressing the "Purge Log Files" button. The table in the bottom section of the "**System and Log Info**" screen contains the disk usage information. The contents of this table are described as follows:

Column Name	Contents
File System	Name of file system that contains the log files.
Total Kilobytes	File system's total capacity in kilobytes.
Used	Amount of file system's total capacity that has been used, in kilobytes.
Available	Amount of file system's currently available capacity, in kilobytes.
Capacity	Percentage of file system's capacity that has been used.

Table 7-9 Summary of Values

PART IV

ISSO

The purpose of this part is to provide security auditing capability to the ISSO. Sections covered in this part are:

Audit Log Maintenance
Archived Logs

Chapter 8

ISSO

The ISSO Interface provides the ability to view, archive, or remove audit information from the Keymaster Sybase Database based on users(s), date/time and audit event. It also allows the ISSO to retrieve previously archived audits. This access is limited to authorized users only. Figure 8-1 shows the **Audit Log Maintenance** page.

Figure 8-1 Audit Log Maintenance Page

From this screen the ISSO may query the system for audit information based upon the criteria provided in the table. A description of each of these criteria follows:

Parameter	Description
User:	The user account being queried for audit information. DEFAULT: Blank; indicates all user accounts are being queried for audit information.
Start Date:	The start date/time of the audit information being

	queried.
	DEFAULT: Current date/time; if **Start Date**
End Date:	The end date/time of the audit information being queried.
	DEFAULT: Current date/time; if **Start Date**
Event:	The audit event being queried.
	POSSIBLE ENTRIES: All Events, Added DAC, Added Group Member, Added New Source, Added User Privileges, Admin Lock, Admin Unlock, Audit Dump, Deleted Audit, Gatekeeper Started, Gatekeeper Stopped, Got Audit Report, Modified Element, Query, Removed DAC, Removed Source, Removed User Privileges, Set Source Parameter, Set User DAC, Transfer Request, User Logger In, User Logged Out
Archive File Name:	Name of file to contain audit records being archived. (The directory path is **not** included in the filename.)
	PURPOSE: Needed only when using the "**Archive Records**" feature.

Table 8-1 Query Parameters

The function of the buttons in the bottom button bar are described as follows:

Button Name	Function
Audit Report	Request an audit report for viewing based on the query parameters selected in the parameter table. If the query is successful, the audit report can be viewed by clicking the "**View Audit Report**" link located below the parameter table.
Archive Records	Archive the records returned from the query based on the parameters selected in the parameter table. The returned records are stored in the file indicated in the "**Archive File Name**" field of the parameter table. (This field contains only the filename and should **not** contain the directory

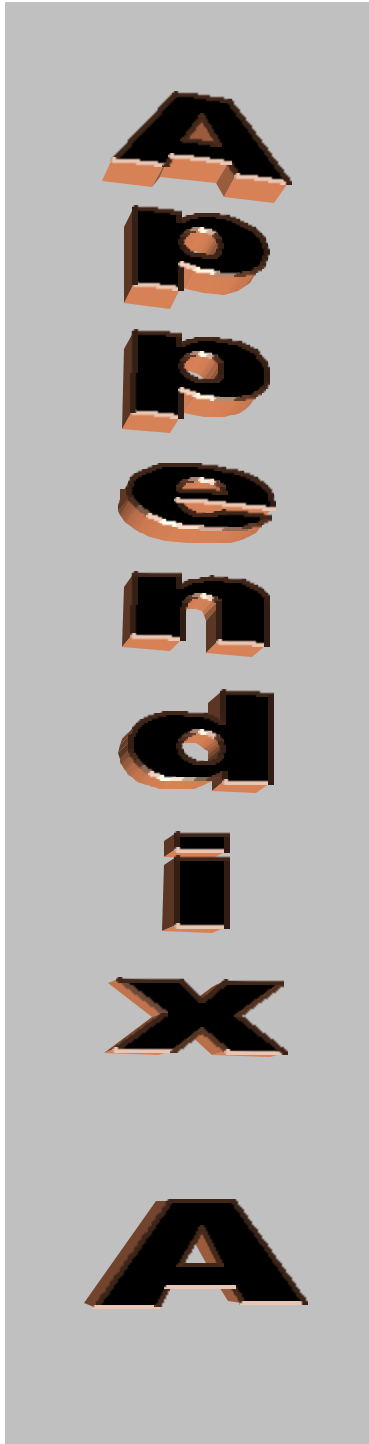|	path. The directory where the archive file goes is "/opt/bswd<version_number>/audits".)
Remove Records	Remove the records from the Keymaster Sybase Database that are returned from the query based on the parameters selected in the parameter table. Upon clicking this button, a verification warning message appears below the parameter table, requesting the administrator to click the "**Remove Records**" button a second time to complete the "**Remove Records**" request.
Reset	Returns the selections to their previously applied values.

Table 8-2 Button Functions

Appendix A
Test Cases

- General
- System Administrator

<table>
<tr><td colspan="4" align="center">Site Acceptance Test – Test Case 1</td></tr>
<tr><td colspan="4">Test Procedure Name :   Keymaster V2.0, General</td></tr>
<tr><td colspan="4">Objective: Test For General Functions in Main. Examine Each Page for Content, Legibility, Grammar and Correctness</td></tr>
</table>

Step	Operator Input	Expected Results	Comments
1	Log into your workstation. Method will vary by workstation type.	User will be logged into workstation.	Login
2	On your workstation, start the browser. Method will vary by workstation type.	The browser will open in a separate window.	Browser
3	In the Browser window, in the Location area, enter the URL for Keymaster protected server and press Enter.	The Keymaster Welcome page will be displayed.	Welcome
4	In the Username box, enter a new user account name and valid password, then click on "**Accept**".	The Keymaster General page will be displayed with Registration blocks to be filled in.	Login
5	Click on "**Support**" in the top frame.	The "Project Broadsword Points of Contact" page will be displayed in a separate window	Support
6	Close the Support window by choosing "**Close**" under the file menu.	The Support window will close. The Preferences-General page will still be displayed.	
7	Click on "**Feedback**" in the top frame.	The Feedback form will be displayed in a separate window. All entries should be blank	Feedback
8	Close the Feedback window by choosing "**Close**" under the File menu.	The Feedback window will close. The Preferences - General page will still be displayed.	
9	Click on "**About**" in the top frame.	The "Project Broadsword" page will be displayed.	About
10	Close the Project Broadsword window by choosing "**Close**" under the File menu.	The Project Broadsword window will close. The Keymaster General page will still be displayed.	
11	Close the Feedback window by choosing "**Close**" under the File menu.	The Feedback window will close. The Preferences - General page will still be displayed.	
12	Click on "**Logout**" in the top frame.	A window will appear asking if the operator is sure he/she wants to end the session.	Logout
13	Click on "**Yes, Logout**".	User will be logged out and the Welcome page will be displayed.	

<table>
<tr><td colspan="4" align="center">Site Acceptance Test – Test Case 2</td></tr>
<tr><td colspan="4">Test Procedure Name :   Keymaster V2.0, System Administrator</td></tr>
<tr><td colspan="4">Objective: Site acceptance for administrative and access control functions</td></tr>
<tr><td>Step</td><td>Operator Input</td><td>Expected Results</td><td>Comments</td></tr>
<tr><td>1.</td><td>Log into your workstation. Method will vary by workstation type.</td><td>User will be logged into workstation.</td><td>Login</td></tr>
<tr><td>2.</td><td>On your workstation, start the browser. Method will vary by workstation type.</td><td>The browser will open in a separate window.</td><td>Browser</td></tr>
<tr><td>3.</td><td>In the Browser window, in the Location area, enter the URL from Keymaster Protected Server and press Enter.</td><td>The Keymaster Welcome page will be displayed.</td><td>Welcome</td></tr>
<tr><td>4.</td><td>Click on "Feedback" on the left side of the frame.</td><td>The Feedback form will be displayed in a separate window. All entries should be blank.</td><td>Feedback</td></tr>
<tr><td>5.</td><td>Close the Feedback window by choosing "Close" under the File menu.</td><td>The Feedback window will close. The Main page will still be displayed.</td><td></td></tr>
<tr><td>6.</td><td>With the Username and Password box blank, click on "Accept".</td><td>The system will display an invalid login message.</td><td>Client prevents login</td></tr>
<tr><td>7.</td><td>With the Username box blank, enter a valid password, then click on "Accept".</td><td>The system will display an invalid login message.</td><td>Client prevents login</td></tr>
<tr><td>8.</td><td>In the Username box, enter a valid user name with a blank Password, then click on "Accept".</td><td>The system will display an invalid login message.</td><td>Conan prevents login</td></tr>
<tr><td>9.</td><td>In the Username box on the browser, enter the same valid user name and an invalid password in the Password box then click on "Accept".</td><td>The system will display an invalid login message.</td><td>Conan prevents login</td></tr>
<tr><td>10.</td><td>In the Username box on the browser, enter the same valid user name and the first 6 characters of the valid password then click on "Accept".</td><td>The system will display an invalid login message.</td><td>Conan prevents login</td></tr>
<tr><td>11.</td><td>In the Username box, enter the same valid user name and a valid password in the Password box, then click on "Accept".</td><td>The system will indicate that the user is locked out due to more than 3 unsuccessful logins</td><td>System admin. will have to unlock user account</td></tr>
<tr><td>12.</td><td>In the Username box, enter a user name and password, which have Administrative and ISSO privileges, then click on "Accept".</td><td>The Search Tools page will be displayed if it was previously selected as the default. On the left side of the page, Administration and ISSO functions should be listed beneath searching functions.</td><td>Login</td></tr>
<tr><td>13.</td><td>In the frame on the left side of the page, under "Administration", click on "User Maintenance".</td><td>The "User Maintenance" page will be displayed.</td><td>User Maintenance</td></tr>
<tr><td>14.</td><td>Enter a current user, then click on "Execute".</td><td>Current and possible privileges of user will be displayed.</td><td></td></tr>
<tr><td>15.</td><td>Make the desired changes utilizing the check boxes, then click on "Execute".</td><td>Page redisplays with user's current and possible privilege status.</td><td></td></tr>
</table>

16.	In the frame on the left side of the page, under ISSO, click on "**Audit Logs**".	The Audit Log Maintenance page will be displayed. There will be a box for User and for Archive File Name. The Start Date and End Date should be the same.	Audit Logs
17.	Enter the user name from step 6 in the "**User**" field, Choose the appropriate Date and Time, then click on the "**Audit Report**" button.	An appropriate audit report will be created for the desired users, dates, and events. A Hypertext line will be displayed "View Audit Report?"	Audit Report
18.	Click on "**View Audit Report?**"	An audit report will be displayed in a separate window. Verify that the invalid logins and the changes that were made are contained in the audit report.	View Audit Report
19.	Close the audit window by choosing "**Close**" under the File menu.	Audit Logs page will be displayed.	
20.	In the frame on the left side of the page, under "**Administration**", click on "**System Config**".	The "System Configuration" page will be displayed.	System Config
21.	In the frame on the left side of the page, under "**Administration**", click on "**Start Registration**".	The "Start Registration" page is displayed.	Start Registration
22.	In the frame on the left side of the page, under "**Administration**", click on "**View Gatekeepers**"	The "View Gatekeeper" page is displayed	View Gatekeeper
23.	In the frame on the left side of the page, under "**Administration**", click on "**System Status**"	The "System Status" page is displayed	System Status
24.	Click on the "**Gatekeeper Config**" tab.	The Gatekeeper Config page will be displayed.	Gatekeeper Config
25.	Under the "**Edit Gatekeeper**" banner, set the "**Client Idle Timeout**" your site's standard value, then click on "**Save**" or leave at default setting	The Gatekeeper Config page will be redisplayed with the new value.	Change Timeout
26.	If Client Idle Timeout changed then save the file and Re-start Conan by doing the following: **If root is using/bin/sh:** **Ps-ef| grep conan** **Kill –9[whatever PID conan has]** **/opt/keymaster2.0/client/bin/startconan**		
27.	Browser must be left idle for Client Idle Timeout value.		
28.	Return to browser and select any new page	Client Idle Timeout Warning is displayed	
29.	On the Keymaster page, click on "**Logout**" in the top frame.	A window will appear asking if the operator is sure he/she wants to end the session.	Logout
30.	Click on "**Yes, Logout**".	User will be logged out and the Welcome page will be displayed.	
31.	On the browser File menu, click on **Exit**.	The browser will terminate.	End of test case

Appendix B
Changing
Password

Changing Sybase Dataserver Administrator (sa) Password

su-sybase<cr>
/bin/csh<cr>
setenv SYBASE <Keymaster Sybase Home Dir><cr>
setenv DSQUERY <Keymaster Sybase Server Name><cr>
${SYBASE}/bin/isql-Usa-P<Sybase sa Passwd>-y${SYBASE}<cr>
1> sp_pasword "<current password>","<new password>"<cr>
2> go <cr>
Password correctly set.
(return status = 0)
1>quit <cr>

If the Sybase "sa" password is NULL (immediately after Keymaster
installation), then replace the sp_password command above with the
following:

sp_password null,"<new password>"<cr>